Implementing an Operational Risk Management Framework at BNP Paribas Lisbon: A Case Study

Siury Geisy Mercedes

Confidential Document

Dissertation for the
Masters in Finance

Advised by

Júlio Fernando Seara Sequeira da Mota Lobão

2016

Biographical Synopsis

Siury Geisy Mercedes was born on the 25th of February in 1988 in the Dominican Republic. She studied International Business and Management in the United States at Dickinson College where she subsequently graduated from with a Bachelor of Arts degree in 2009. After graduating, Siury acquired work experience in the United States, Spain and France, where she also expanded her language skills. In 2014, she was accepted into the Faculty of Economics at the University of Porto and the Quantitative Techniques for Economics and Management (QTEM) network. During her time in Porto, Siury was a member of the FEP Finance Club as a Financial Markets Analyst, where she contributed by reporting events impacting the financial markets on a daily basis. As a QTEM student, she obtained a unique learning experience to further her international and cultural exposure through studying at the BI Norwegian Business School in Oslo, Norway in the spring semester of 2015.

In December 2015, Siury obtained the opportunity to partake in a nine month internship in Lisbon as an Operational Risk Analyst Trainee within the Front Office Global Markets Operational Permanent Control team at BNP Paribas Corporate and Institutional Banking. In this role, she aided her team in implementing control plans that could help identify and reduce or eliminate the potential operational risks that the bank faced. This work experience paved the way for this dissertation.

Acknowledgements

It takes a village to write a thesis.

I would like to first express my gratitude to Júlio Lobão, my advisor and professor at the Faculty of Economics at the University of Porto, for his continual support, guidance and helpful feedback throughout the process of developing my dissertation. His timely advice, dedication, knowledge and scrutiny of my work helped me deliver my best work possible.

Of course, this study would not have been possible without the opportunity and experience gained at BNP Paribas. I am grateful for the privilege to be a part of such an elite financial institution and for the knowledge obtained from the inspiring group of people that work at the bank. I am also grateful to my manager at BNP Paribas, Dany Costa, who introduced me to the topic, and the Head of the Global Markets Front Office team, Christopher Claude, for accepting my dissertation proposal.

I would like to give a special thanks to my OPC team members, Marta Brito Da Silva and Francisco Valerio, for guiding me throughout the development of the operational risk management framework, providing me with their expertise, supervising my project, and advising me throughout the entire process. Their time and efforts greatly contributed to my ability to accomplish this dissertation.

I would like to also thank the rest of my colleagues who patiently allowed me to shadow them and pester them with questions as they performed their processes in order for me to analyze and understand their tasks. Thank you to my family, specifically my mother and fiancé, for helping me get through the stressful periods and for continually encouraging me in order for me to push through. I am blessed to have such a strong support system.

It took a village to write this thesis and I am eternally grateful to all of the people and organizations that supported, encouraged and guided me throughout the process. This study truly would not have been possible without each of their contributions. Thank you.

Abstract

Since risk will always pose a threat of destabilization to financial institutions, an effective operational risk management system is essential for banks. Banks must ensure that the risks that could potentially have any significant impact could be detected and mitigated as early as possible in order to protect the interests of the company's stakeholders. This study analyzes whether an operational risk management model was relevant to the BNP Paribas Global Markets Lisbon team through analyzing the team's processes and the potential risks associated to those processes. If the model was in fact necessary, the objective was to develop a sound operational risk management model that would function to mitigate those identified risks. Ultimately, we find that there was, indeed, a need to implement an operational risk model to reduce or avoid the potential impact of the detected risks. This study fills a part of the research gap in that it provides a glimpse of the process of developing and implementing an operational risk and permanent control management structure at BNP Paribas Lisbon. Through identifying, evaluating and measuring the presence of operational risk, we established a risk map and designed an internal control system, as it pertained to the Global Markets Lisbon team, in order to foster a system that continually and systematically reduces the financial, reputational, and/or operational impact of these potential risks.

Key-words: Operational Risk, Risk Management, Investment Banking, Control Plan
JEL Classification: G20, G21, G24, G28

The information portrayed in this report has been obtained from public sources and do not contain any sensitive data or information of the BNP Paribas Group. The examples, names and figures used are purely for illustrative purposes and are not to be relied on in any way as a reflection of BNP Paribas' activities, personnel, or data.

The work experience allowed the author to understand the operational and analytical aspects of the process surrounding operational risk management and as such the author intended this work project to do the same for its recipients. The views and conclusions expressed in this work project are solely that of the author and do not reflect that of BNP Paribas Group, their affiliates or its personnel.

Resumo

O risco representa uma ameaça constante de desestabilização das instituições financeiras. Desta forma, um sistema de gestão de risco operacional eficaz é essencial para o bom funcionamento dos bancos. Os bancos devem assegurar que os riscos que podem potenciar impactos significativos sejam detectados e mitigados o mais cedo possível, a fim de proteger os interesses dos *stakeholders* da empresa. Esta dissertação tem como objectivo analisar a aplicação de um modelo de gestão de risco operacional na equipa de Global Markets do BNP Paribas – Lisboa, e avaliar a sua relevância através da análise das tarefas realizadas pela equipa e dos potenciais riscos associados à sua actividade. Se o modelo for realmente necessário, o objectivo será desenvolver um modelo de gestão de risco operacional forte de forma a mitigar os riscos identificados. Em última análise, os resultados mostram que existia de facto a necessidade de implementar um modelo de risco operacional para reduzir e/ou evitar o potencial impacto dos riscos detectados. Este estudo preenche uma parte da lacuna na investigação uma vez que oferece um vislumbre do processo de desenvolvimento e implementação da gestão de risco operacional e estrutura de controle permanente na equipa de Global Markets do BNP Paribas Lisboa. Através da identificação, avaliação e quantificação da presença de risco operacional, foi estabelecido um mapa de risco que projetou um sistema de controlo interno, a fim de promover um sistema contínuo e que progressivamente vai reduzindo o possível impacto financeiro, reputacional e/ou operacional desses mesmos riscos identificados.

Palavras-chave: Risco operacional, Gestão de Riscos, Investimento bancário, Plano de controle

Classificação JEL: G20, G21, G24, G28

As informações retratadas neste relatório foram obtidas a partir de fontes públicas e não contêm quaisquer dados sensíveis ou informação do grupo BNP Paribas. Os exemplos, nomes e valores numéricos são utilizados apenas para fins ilustrativos e não deverão ser invocados de forma alguma como um reflexo das actividades, pessoal ou dados do BNP Paribas.

A experiência de trabalho permitiu ao autor compreender os aspectos operacionais e analíticos do processo em torno de gestão de risco operacional e, como tal, o autor pretendeu com este projecto, transmitir o mesmo aos seus destinatários. As opiniões e conclusões expressas no presente projeto de trabalho são únicas do autor e não reflectem as do BNP Paribas Group, suas afiliadas ou do seu pessoal.

Table of Contents

Index of Tables

Index of Figures

Acronyms

ABD	ARIS Business Designer
AMA	Advanced Measurement Approaches
ARCM	ARIS Risk & Compliance Manager
BCBS	Basel Committee on Banking Supervision
BCD	Business Control Diagram
BEICFs	Business Environment and Internal Control Factors
CIB	Corporate and Institutional Banking
EI	Exposure Indicator
EL	Expected Loss
EPC	Event Process Chain
FXLM	Forex and Local Markets
HoD	Head of Desk
HoF	Head of Filiere
ILD	Internal Loss Data
LDA	Loss Distribution Approach
OPC	Operational Permanent Control
PE	Probability of Loss Event
RAROC	Risk adjusted return on capital
SBA	Scenario Based Approach
VACD	Value added chain diagram

Chapter I

1. Introduction

Risk is a persistent encumbrance that consistently casts an ominous threat to a financial institution's stability. Risk can emerge in many forms, market, credit, and operational to name a few, and can strongly undermine a financial institution's ability to sustain a steady progression of economic growth. In order to maneuver through the unpredictable and potentially perilous risks, financial institutions are required to develop systems that keep them cognizant of the level of risks that they are exposed to, as well as a capital buffer that would protect them against unanticipated losses.

However, several of these systems emerged only after numerous financially catastrophic incidents called attention to the need for banks to improve their level of protection against risks. In 2008, several interconnected risks were within the epicenter of the mortgage backed securities that ignited a global financial crisis. In the early 2000s, several banks began strategically bundling mortgage loans and selling them as securities to investors in order to profit from a boom in the housing market, though, largely neglecting the looming credit risk. As interest rates rose so did the number of defaulted loans, which consequently increased the liquidity risk of all the banks involved. Lehman Brothers, the fourth largest investment bank in the United States at the time, was significantly impacted by these risks reporting a quarterly loss of $3.9 billion in September 2008 and ultimately filing for Chapter 11 bankruptcy, one of the largest in U.S. history (Ferrell *et. al*, 2010). Lehman Brothers' collapse sent shockwaves throughout the global financial markets and was a large factor in what culminated into a severe global recession.

In 2014, BNP Paribas, a global financial institution, was fined $8.97 billion for transactions conducted through the US financial system on behalf of Iranian, Sudanese, and Cuban entities, which were subject to U.S. economic sanctions (Kittrie, 2016). The Department of Justice stated that BNP Paribas had organized various elaborate schemes that were intended to deliberately mask their illicit transactions from U.S. regulators

(Kittrie, 2016). The financial penalty was reportedly the largest criminal fine ever imposed by the U.S. government.

In the case of the Lehman Brothers collapse, a year prior to its downfall, management had accepted a large increase in their risk appetite limit in order to meet their ambitious growth strategy (Engelen, 2011). The bank's excessive risk taking led it to have a leverage ratio that could not sustain the market illiquidity that arose from the mass defaults, which produced huge unanticipated losses for Lehman Brothers. The drastic losses and large leverage ratio damaged the bank's reputation and made it difficult for the bank to obtain funding that would sustain their day-to-day operations. By this point, it was a colossal domino effect that would ultimately lead to the bank's demise. At the root of this downward spiral is an operational error that could have been avoided had there been effective operational risk management systems that weighed the potential consequences of a larger risk appetite.

BNP Paribas' case is an example of operational risk that ultimately proved costly to the bank. Operational risk involves the actions of the firm, its entities and its staff, which can lead to negatively impacting the reputation of the financial institution, as well as, investor confidence in the financial system. Both scenarios portray that it is pertinent for banks to adopt behaviors, practices, internal controls, and governance mechanisms that would prevent or reduce the imminent risks that can potentially have catastrophic consequences. Risks will always threaten to undermine a financial institution's stability; however, it is ultimately the responsibility of these banks to enhance their operational risk management systems in order to better protect themselves against adverse events that could prove disastrous to its reputation, operation and finances.

The objective of this study is to determine if an operational risk model is applicable to the BNP Paribas Global Markets Lisbon team. If it indeed is applicable, the second objective is to develop a sound operational risk management model for mitigating those identified potential risks. In order to develop a tailored operational risk model, we conduct an internal analysis of the processes performed by the teams in Lisbon. It is important to understand the processes performed by each team member in order to identify the risks, if any, involved in their procedures.

Ultimately, we determine that there was a need for the operational risk model to include some of the teams in Lisbon. Thus, we proceed with developing systematic procedures that will help reduce or avoid any potential risks. In order to develop a customized operational risk management system, we first construct a risk map that gauges the risks associated with particular processes performed by the Global Markets Lisbon team. Along with the risk map, we develop a control plan, in which the goal is to mitigate the potential impact of that particular risk. The frequency and a clear objective of the controls is defined and established according to the specific process. Therefore, the goal of the study is also to portray the various stages of building an operational risk management model that respects the standards imposed by the Basel Committee. To the best of our knowledge, this is the first study to describe these procedures as it pertains to BNP Paribas. Thus, this study provides a glimpse, however small, of BNP Paribas' operational risk management processes.

In the following chapter, we will discuss the Basel Committee, which was formed to develop regulatory standards intended to synchronize procedures of protecting against operational risk for all banks. We explain operational risk and the components that make up an effective operational risk management structure. Additionally, we provide a general overview of the risk management procedures that many banks have or should have implemented through the regulatory reforms established by the Basel Committee. In chapter three, we discuss the proposed calculation methods as set by the Basel Committee, as well as the most popular methodological approaches used among banks following the Basel Committee regulations. In chapter four, we delve into the analysis conducted within BNP Paribas, the organizational structure of the business and the process of developing a risk map and the subsequent control plan implementation. We explain in detail the internal control design, systems, procedures and processes that were created in order to mitigate the risks detected through the risk mapping process. We then discuss notable operational risk incidents that have highlighted the importance of an efficient operational risk management framework. In chapter five, we conclude.

Chapter II

2. Literature Review

In this chapter, we will discuss the origins of the Committee that formed in order to enhance financial stability globally through preventing or diminishing the impact of the risks that had previously led to global crisis. The Committee aims to address these risks through introducing consistent risk management standard frameworks that fortify the regulatory system, supervision and practices of banks worldwide.

The section following the introduction of the Committee explains the definition of operational risk and the purpose of developing an operational risk management system. The section thereafter presents the very first framework established by the Committee, the Basel I. The Basel I section delves into the standards set forth within the original structure as well as the criticisms that it faced. Thus, the subsequent section discusses the second revised framework, the Basel II, which aims to correct the ambiguities found within the Basel I. The last section explains the categories that the Basel Committee established in order for banks to identify the types of events or risks that banks face and that could negatively impact that entity.

2.1 Regulatory Origins

The Basel Committee on Banking Supervision was born out of the international financial cataclysm that transpired in the 1970s due to the collapse of the Bretton Woods system in 1973 (BCBS, 2015). The financial market pandemonium led to several international banks incurring hefty foreign currency losses and for some permanently closing down (BCBS, 2015). Consequently, the central bank governors of the G10 countries took proactive measures in response to the financial market turmoil and the

banks' precarious position by establishing the Basel Committee on Banking Supervision (BCBS) at the end of 1974 (BCBS, 2015). The Committee was envisioned as a forum for systematic collaboration amongst its participating countries on banking supervisory matters and intended to improve financial stability through setting minimum standards for financial supervision and regulation of banking worldwide (BCBS, 2015).

Although the Committee's decisions have no legal power, the Committee began, in 2012, monitoring the execution of their supervisory standards and guidelines of its members to help advance the global banking system, stimulate public confidence and foster a fair regulatory system for internationally active banks (BCBS, 2015). The Committee is currently comprised of twenty-eight jurisdictions; central banks represent their corresponding countries and the authority with formal responsibility for the prudential supervision of banking business acts for the jurisdictions without a central bank (BCBS, 2015).

2.2 Operational Risk

The Basel Committee defines Operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" (BCBS, 2001). Therefore, according to the definition, there are four potential causes of operational risk: people, processes, systems and external events. The definition also includes legal risk, but disregards reputational and strategic risk (BCBS, 2001).

Alexander (2003) best explains operational risk as comprising of all possible losses originating from operational inputs, internal processes and systems (including employees and equipment), downstream supply chain partners or customers, and external events. An efficient operational risk management framework should take into account all financial impacts even gains and near-misses in addition to losses and opportunity costs. Near-misses simply mean that the loss did not occur but it is important to record it because should the

event reoccur it does not necessarily mean that it would result in a near-miss again (BCBS, 2011).

The goal of an operational risk management framework is to identify any malfunctioning and/or risks that an entity may be exposed to, and ultimately, if feasible, thwarts their occurrence or represses the financial ramifications. There is also the regulatory aspect in that banks are required to declare all significant incidents to regulators. Lastly, the operational risk identification helps banks ensure that they have the necessary capital reserved for the worst-case scenario for operational risk (BCBS, 2011).

2.2.1 Basel I

Following the Latin American debt crisis in the 1980s, the Committee noticed a need for sturdier capital ratios and, thus, developed their first framework now referred to as Basel I (BCBS, 2015). The goal was to develop capital standards that would consolidate the measurement of capital adequacy for their banking systems worldwide.

The Basel I set a minimum capital ratio of capital to risk weighted assets of eight percent (BCBS, 2008). Ultimately, this accord was implemented not only in the member countries but also in almost all countries with active international banks, which essentially removed competitive inequality due to differences in national capital requirements. The document was repeatedly modified throughout the 1990s but one important alteration was the Market Risk Amendment (BCBS, 2015). The Market Risk Amendment added a capital requirement for the market risks banks are exposed to into the framework, which up until then solely addressed credit risk (BCBS, 2015). Subsequently, for the first time, banks were able to incorporate value-at-risk models, in addition to other quantitative parameters and qualitative standards, to assess their market risks and meet their market risk capital requirements (BCBS, 2015).

Overall, the Basel I was executed fairly effortlessly amongst the Basel Committee jurisdictions, except for Japan, which took a bit longer to effectuate the accord due to suffering a banking crisis in the late 1980's that hampered its ability to swiftly implement the Basel I (Balin, 2008). Notwithstanding its rather smooth implementation, Basel I is not

free of criticism on account of several observed limitations. One main criticism is that although the accord recognized that banks must protect itself against other kinds of risk, Basel I only addressed the credit risk its member G-10 states, all developed markets, were potentially exposed to (Tarullo (2008), Balin (2008)). Therefore, Basel I not only excluded banks operating outside of developed markets from its scope, but also focused on one sole risk, essentially leaving banks exposed to a wide spectrum of risks. Another criticism was the generality and absoluteness of the standards that left a chasm in Basel I's risk weightings and allowed banks to maneuver around the benchmarks in order to acquire higher risks than what was originally designed by the Basel I (Balin, 2008). These shortcomings led the Basel committee to acknowledge a demand for an enhanced framework that could better ensure ample financial stability in the international financial system (Balin, 2008). Consequently, revisions of the Basel I ultimately yielded the Basel II.

2.2.2 Basel II

The Basel Committee introduced a revised version of the Basel I in 1999, commonly referred to as Basel II, which was meant to rectify some of the loopholes found in the original framework (BCBS, 2015). Basel II further expands the "pillar" framework established in Basel I in order to broaden the scope, technicality, and dimensions of the Basel Accord (Balin, 2008). The Basel II is founded on three pillars:

I. Minimum Capital Requirements
II. Supervisory Review
III. Market Discipline

The minimum capital requirements pillar is comprised of three components: the delineation of regulatory capital, risk-weighted assets, and the minimum ratio of capital to risk-weighted assets (Balin, 2008). The risks have been categorized as follows:

1. Credit risk
2. Market risk

3. Operational irsk
4. Liquidity risk
5. Legal risk

Basel II clearly defines separate minimum capital requirements for operational risk. For operational risk, a bank has the flexibility to build internal models to assess the bank's operational risk profile and determine the minimum regulatory capital requirements.

The second pillar, Supervisory review process, puts an emphasis on the supervision of the bank's capital adequacy, externally and internally (Balin, 2008). The overall arching principal is that banks must oversee all operational risk events and have internal risk management systems that are ethical and transparent to banking supervisors. Not only would this system help identify and understand past and potential future operational risk events but also would help a bank spot preventable risks or areas of mitigating the impact.

Market discipline, the third pillar, encourages banks to disclose what previously was only available to regulators, such as a bank's risk exposures, capital, risk assessment processes, etc. (Tarullo, 2008). Under Basel II's standards, it is recommended that banks release quarterly statistics related to the aggregate amounts of surplus capital (both Tier 1 and Tier 2) the bank holds, risk-weighted capital sufficiency ratios, reserve requirements for credit, market, and operational risk, and a complete explanation with expectations of the risk reduction methods the bank has (Tarullo, 2008). By having the information available to the public, Basel II hopes to endow shareholders with the ability to compel banks to take particular restraints in their risk taking actions and their reserve holding approaches (Balin, 2008). In this way, if a bank is taking huge risks but has proportionally few reserves then shareholders could take action and punish these banks for doing so.

Current events and criticism of the Basel II have shown a profound need for an updated Basel framework even prior to the collapse of the Lehman Brothers in September 2008. Consequently, the Basel III was released relatively recently but has yet to be implemented by all banks (BCBS, 2015). Since many banks are still currently implementing the Basel II accord and have up until 2018 to switch to Basel III, the scope of this research has been restricted within the Basel II framework.

2.3 Operational Risk: Basel event types

The Committee categorized seven Level 1 event types nomenclature, which are the types of incidents that will be used to calculate operational risk (BCBS, 2006). Defining an event is critical to analyzing its impact as well as the likelihood of it occurring again, particularly for the frequency/severity approach. The Basel regulations demarcated these even type levels; however a bank could feel free to implement an internal sub-level if it saw it appropriate.

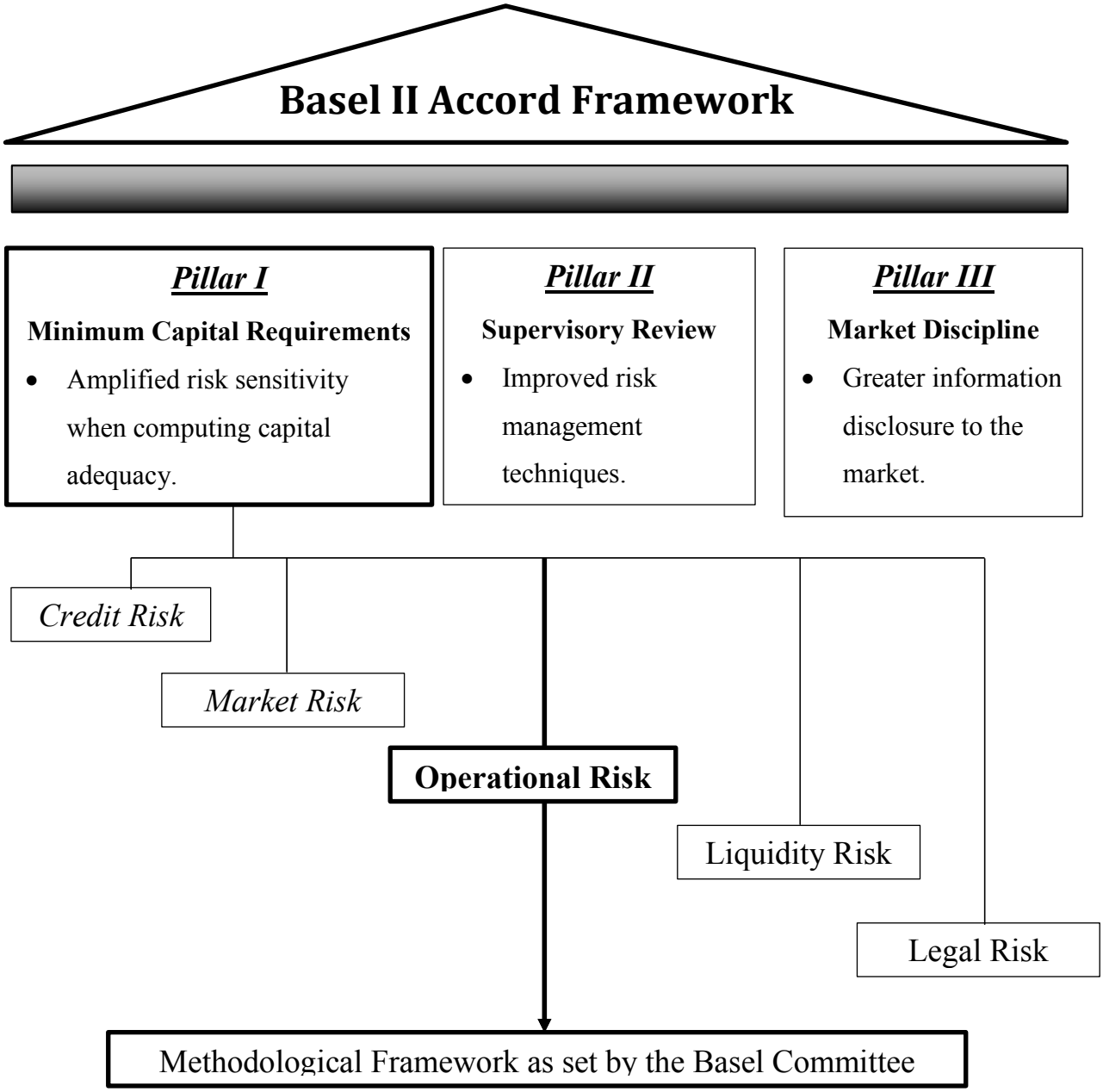
The level 1 event types are:

1. Internal fraud
2. External fraud
3. Employment practices and workplace safety
4. Customers, Products and Commercial Practices
5. Damage to physical assets
6. Business disruption & system failures
7. Execution, delivery and Process Management

To further clarify the event types, the following are some examples and/or explanations for each of the event types that could occur. Although the definition of fraud varies, it essentially revolves around some sort of deception that has intentionally been committed (Shevchenko, 2011). Internal fraud would entail falsification of information from a staff member such as tax evasion, money laundering and embezzlement (Shevchenko, 2011). External fraud, as the name implies, are external factors such as an outside party forging documents, hacking, and stealing internal information (Shevchenko, 2011). Employment practices and workplace safety would encompass any sort of discrimination, or actions that could lead to a lawsuit for example (Shevchenko, 2011). Customers, Products and Commercial Practices deal with market manipulation, breach of market rules, or improper trades, etc. Damage to physical assets would include terrorist attacks that affect the company, vandalism, or natural disasters (Shevchenko, 2011).

Business disruption and system failures would be anything that causes an employee to not perform the necessary processes for the job, such as IT issues (Shevchenko, 2011). Lastly, execution, delivery and Process Management is anything that deals with the actual execution of processes, such as inserting the wrong data, accounting errors, or losing a client's assets (Shevchenko, 2011). The figure below summarizes the Basel II Accord Framework and portrays the scope of this research as it pertains to the framework.

Figure 1: Basel II Framework



Chapter III

3. Methodological Framework

This chapter discusses the methodological framework that the Basel Committee established for banks to compute the capital buffer needed to cover events that could lead to unexpected losses for the bank. After the proposed calculation measurements are introduced, we discuss the necessary data elements that the Basel Committee has set as essential for banks to have a comprehensive and effective capital calculation approach. Thereafter, we briefly introduce two popular calculation approaches that banks implementing the third proposed measurement use to compute the necessary capital.

3.1 Basel II: the proposed calculation methods

There are three proposed measurement methodologies for calculating operational risk capital charges. Progressing from complexity and risk sensitivity, they are: the Basic Indicator Approach, the Standardized Approach, and the Advanced Measurement Approaches (BCBS, 2006). The Basic Indicator Approach is denoted as follows:

$$K_{BIA} = [\sum(GI_{1\dots n} \mathrm{x}\, \alpha)]/n \qquad (1)$$

where K_{BIA} is the operational risk capital charge, GI is the annual gross income, where positive, over the previous three years, n is the number of the previous three years for which gross income is positive, and α is 15%, which is a weighting coefficient set by the Basel Committee (BCBS, 2006). Thus, there are no specific eligibility criteria for Banks in this approach and the average Net Banking Income is the only indicator. The weighting coefficient is related to the industry wide level of required capital to the industry wide level of the indicator (BCBS, 2006).

The Standard Approach separates itself from the Basic Indicator Approach in that the former approach determines the amount of cash a bank must have to protect itself through splitting the bank into specific business lines as defined by the Committee (BCBS, 2006). The business lines are stated as follows: corporate finance, trading & sales, retail banking, commercial banking, payment & settlement, agency services, asset management, and retail brokerage (BCBS, 2006). The approach can be expressed as

$$K_{TSA} = \{\sum_{years\ 1-3} max[\sum(GI_{1-8} x \beta_{1-8}), 0]\}/3 \quad (2)$$

where the operational risk capital charge, K_{TSA}, depends on the GI_{1-8}, the annual gross income in a given year, as outlined in the Basic Indicator Approach, for each of the eight business lines, and on a Beta, β_{1-8}, also for each of the eight business lines (BCBS, 2006). The beta is predetermined by the Committee and is weighted against the gross income of each of the eight business lines within the company to assess the level of required capital (BCBS, 2006). The values of the betas, detailed in Table 1, suggest the risk related to the business lines.

Table 1- Standardized Approach Reserve Targets

Business Lines	Beta Factors
Corporate finance (β_1)	18%
Trading and sales (β_2)	18%
Retail banking (β_3)	12%
Commercial banking (β_4)	15%
Payment and settlement (β_5)	18%
Agency services (β_6)	15%
Asset management (β_7)	12%
Retail brokerage (β_8)	12%

Source: BCBS (2006)

Similar to the Basic Indicator Approach, there is only one weighting coefficient: the average Net Banking Income for each business line, over the last three years (BCBS, 2006). However, unlike the Basic Indicator Approach, there are eligibility criteria for the

Standardized Approach. In order to qualify for use of the Standardized Approach, a bank must satisfy the following criteria:

- Its management must be actively involved in the supervision of the operational risk management framework;
- The bank has implemented an operational risk management system
- The bank has implemented a well-organized and documented risk management framework, such as a set of procedures, risk mapping, etc.
- The bank has sufficient funds for the management and maintenance of this framework.

The Advanced Measurement Approach (AMA) allows banks to develop their own internal framework and calculate the necessary reserves for operational risks through taking into account the bank's particular risks (BCBS, 2006). The Standardized Approach criteria also apply in this approach and there must be a review of the model and its documents through an independent audit and a systematic validation by the supervisor (BCBS, 2006). The goal of the AMA is for banks to develop capital reserves that are more pertinent to the bank's actual risk profile (BCBS, 2006).

In order to implement this framework, regulators must eventually approve the final measurement approach (Balin, 2008). Ultimately, the internal models are expected to exhibit precision within the Basel II Accord risk matrix, i.e. the eight aforementioned business lines by the seven event types (BCBS, 2006). The AMA strategy employed should weigh internal operational loss data, external operational loss data, scenario analysis and factors that expose the business environment and the internal control systems through a clear, sound, and verifiable approach (BCBS, 2006).

The loss distribution approach (LDA) and the scenario-based approach (SBA) are the two most popular AMA models used (BCBS, 2011). Although these models differ, there are four data elements in which the underlying principle would be generally valid for either.

3.2 The Four Data Elements

Banks utilizing the AMA are required to use four data elements, which are: internal loss data, external data, scenario analysis, and business environment and internal control factors (BEICFs) (BCBS, 2011). These four data elements would not only provide insight to a bank's risk profile, it would also help with risk quantification, risk management, accounting and other types of reporting. The following sections give a brief description of each of the four data elements, which have been obtained from the Basel 2011 Operational Risk Consultative Document.

3.2.1 Internal loss Data

Out of the four data elements, internal loss data may be the most valuable because it provides a record of the bank's actual losses, thus making it the best representation of the bank's business risk profile and risk management practices (BCBS, 2011). Within the operational risk measurement system, the internal loss data would help in estimating the loss frequencies and, along with the external data, would aid in attuning the severity distribution (BCBS, 2011). The internal loss data offers a base for the bank's scenarios within its own risk profile and also acts as an input into the scenario analysis since it is a bank's actual loss occurrence.

For banks following the AMA standard, The Basel II Framework proposes that banks gather internal data over a minimum period of five years, in order to calculate the capital charge (BCBS, 2011). However, if the bank has just qualified for the AMA standard, then a three-year period of accumulated internal data is acceptable (BCBS, 2011). In any event, many banks' high severity internal loss events are insufficient to inform the tail of the distributions for producing significant evaluations of capital needs (BCBS, 2011). This is where external data and/or scenario analysis are essential.

3.2.2 External Loss Data

External loss data's intended use is to enhance the internal data since it would provide additional information on large losses that particular bank may not have experienced. External data offers insight on the losses experienced in the industry as a whole. Thus, external data can be used to estimate the loss severity since the data contains important information to inform the tail of the loss distributions (BCBS, 2011). Furthermore, external data would serve as supplementary inputs into scenario analysis (BCBS, 2011).

Nonetheless, external data is publicly obtained and as result would have reporting biases embedded in its information (BCBS, 2011). Furthermore, the data is sourced from differing banks and may not necessarily have relevant information for the risk profile of the specific bank utilizing the data (BCBS, 2011). Therefore, each bank should have outlined methodologies for counteracting the biases, evaluating its pertinence and scaling the loss quantities as applicable. Scaling tailors the external data loss amounts to the bank's actual business activities and risk profile.

3.2.3 Scenario Analysis

Differing from internal and external data, scenario analysis provides predictive analysis of events that have yet to happen to expose potential operational risk exposures (BCBS, 2011). Having a strong scenario analysis is a critical component of the operational risk management framework. Using internal data and external data to inform the scenario, the process will be subjective by nature and will contain substantial ambiguities (BCBS, 2011). The output of the model would portray these ambiguities through providing a range for the estimate of the capital requirements (BCBS, 2011). Therefore, scenario uncertainties offer an instrument for estimating a suitable level of caution in deciding the final capital requirements.

Consequently, banks need to establish a strong governance framework that ensures the integrity and consistency of the estimates provided by the scenario analysis. According

to the Supervisory Guidelines for the Advanced Measurement Approaches (BCBS, 2011), in the recognized scenario framework, supervisors will discern the following features:

(a) A clearly defined and repeatable process;

(b) Good quality background preparation of the participants for the scenario generation workshop;

(c) Qualified and experienced facilitators with consistency in the facilitation process;

(d) The appropriate representatives of the business, subject matter experts and the corporate operational risk management function as participants involved in the workshop;

(e) A structured process for the selection of data used in developing scenario estimates;

(f) High quality documentation, which provides clear reasoning and evidence supporting the scenario output;

(g) A robust independent challenge process and oversight by the corporate operational risk management function to ensure the appropriateness of scenario estimates;

(h) A process that is responsive to changes in both the internal and external environment;

(i) Mechanisms for mitigating biases inherent in scenario processes. Such biases include anchoring, availability and motivational biases.

3.2.4 Business Environment and Internal Control Factors

The BEICFs, similar to the scenario analysis, are also forward-looking evaluations that are also subjective, which poses a challenge when integrating into the capital model (BCBS, 2011). BEICFs provide evaluations of business risk factors and the bank's internal control setting (BCBS, 2011).

Generally, there is an established quantification framework and BEICFs are used as an indirect input and as an "ex-post" modification to the model output (BCBS, 2011). This modification could result in an adjustment of a rise or cut in AMA capital charge at a group or business line level. However, due to its subjectivity a bank should have procedures that limit and justify the extent of the adjustment (BCBS, 2011). When compared over a period of time to the ILD, the direction and magnitude of the adjustments should be suitable (BCBS, 2011).

3.3 Internal Measurement Approach

The Internal Measurement Approach aims to integrate the specific bank's internal loss data into the calculation of the required capital (BCBS, 2001). Through the internal measurement approach, individual banks have the power to use their own judgment in deciding how to use their internal data, while supervisors establish the technique for computing the required capital that is uniform. To assure the integrity of the measurement approach, data quality, and the competence of the internal control environment, supervisors would need to enforce quantitative and qualitative standards (BCBS, 2001).

The capital charge for the operational risk of the bank is determined through a set of procedures under the Internal Measurement Approach. First, the activities conducted in the bank need to be separated by business lines, which can be the same as those suggested in the Standardized Approach (BCBS, 2001). Additionally, a cluster of general operational loss types should be delineated and applied across those business lines (BCBS, 2001). Thereafter, a supervisor defines an exposure indicator (EI) for each business line/loss type combination, which serves as a proxy for the size or amount of each business line's operational risk exposure (BCBS, 2001). Then, depending on the bank's internal loss data, two parameters are determined: Probability of loss event (PE), which is the likelihood of the occurrence of loss events and the Loss given that event (LGE), which is the amount or exposure that would be consumed as loss given that event (BCBS, 2001). The product of

these three variables, EI, LGE and PE, would yield the expected loss (EL) for each of the business line/loss type combination (BCBS, 2001).

In order to translate the expected loss into a capital charge, the supervisor supplies a "gamma term" for each business line/loss type combination (BCBS 2001),

$$Required\ Capital = \sum_i \sum_j [\gamma(i,j) * EI(i,j) * PE(i,j) * LGE(i,j)] \quad (3)$$

where i is the business line and j is the risk type, and the γ is a constant that is used to convert the EL into risk or the capital charge (BCBS, 2001). The measure of γ is established and fixed for each business line/loss type by the supervisors (BCBS, 2001).

However, there are several issues that the Committee recognized needed to be resolved within the internal measurement approach. In order for there to be a standard approach globally across banks, there needed to be a consistent method for deciding what constituted as an operational risk loss event (BCBS, 2001). Furthermore, the internal data obtained may not necessarily truly represent the bank's risk profile.

3.3.1 The Loss Distribution Approach

The LDA is a popular and more advanced version of the "internal methodology" that also satisfies the AMA standards (BCBS, 2011). Using the LDA, banks can calculate the probability distributions for the operational risk losses for each business line or event type over the period of one year (Shevchenko, 2011). Each bank can and should customize their LDA measures around their entities related risks but it is also important that they fall within the regulatory guidelines.

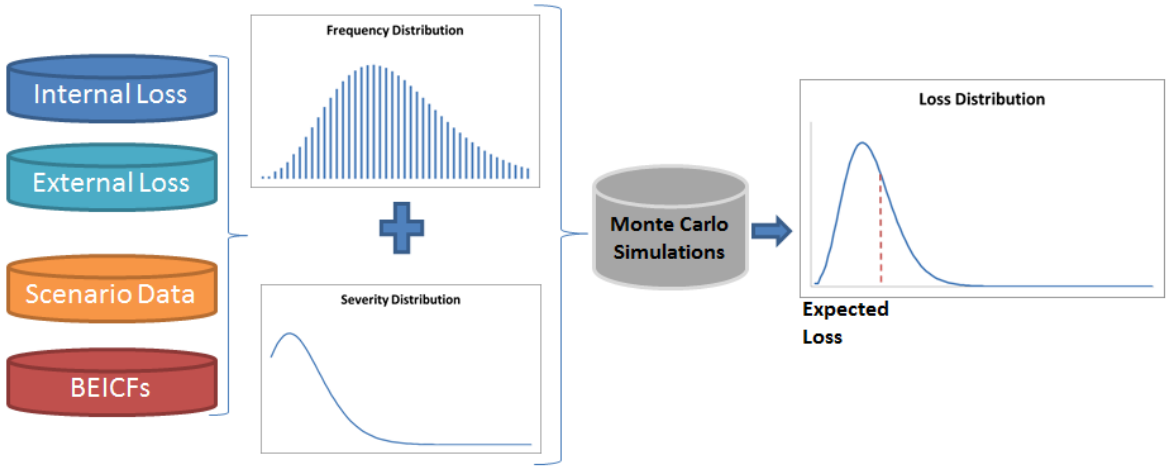
Frachot *et al.* (2001) describes step by step how to reconcile quantitative and qualitative aspects of the data in order to implement the Loss Distribution Approach in practice. According to Frachot *et al.* (2001) there are five steps to implementing the LDA:

- Severity Estimation
- Frequency Estimation

- Capital Charge Computation
- Confidence Interval
- Self-Assessment and Scenario Analysis

The severity is, in regards to financial loss, the impact of the event whereas the frequency is the number of loss events that occurred within a certain time period (Alexander, 2003). The severity estimation is a calibration of the impact of each event that takes into account the complexities of the existing reporting bias in the data (Frachot *et al.*, 2001). Once the bank has established the severity distribution and the frequency distribution then an empirical approximation of the total loss distribution could be determined through Monte Carlo simulation, which is the capital charge (Frachot *et al.*, 2001). Since the capital charge is an estimation, the confidence interval is a tool used to justify the computed capital charge (Frachot *et al.*, 2001). The Self-Assessment and Scenario Analysis are the same as the Scenario Analysis and BEICFs that had been previously discussed.

Figure 2: Loss Distribution Approach



Dutta and Perry (2007) take a different approach by first understanding how to appropriately measure operational risk rather than evaluating whether certain techniques can be used for a particular institution. This is important because institutions typically use the results of their operational risk measurements to estimate the capital to hold as reserves

for possible operational losses. This means that the measurements used should accurately capture the actual risk exposures that the institution is vulnerable to. Dutta and Perry (2007) evaluated the frequently used methods, found them to be inadequate in regards to the goodness-of-fit tests effectuated and thus introduced a new technique that they found to perform insurmountably better than the other models they tested. The new technique, g-and-h distribution, modeled the whole severity range with one distribution and fit the data and results providing reliably realistic capital estimates.

Chapelle *et al.* (2008) analyze the main obstacles banks face when implementing the AMA to evaluate operational risk. They studied four categories of two business lines, "Asset management" and "Retail banking", and two event types, "Clients, products and business practices" and "Execution, delivery and process management", of a large financial institution. They developed a matrix where in each cell they calibrated two truncated distributions functions. One distribution function described the "normal" losses and the other portrays the "extreme" losses. Through examining the risk adjusted return on capital (RAROC) to understand how operational risk management influences bank profitability, Chapelle *et. al* (2008) found that active management techniques would result in significant savings for the bank.

Table 2: Methodological Approaches to Capital Estimation

Approaches	Methods	Results	Studies
Search for how to appropriately measure operational risk prior to choosing a technique.	Use a new technique: g-and-h distribution	New model provides reliably realistic capital estimates that are superior to estimates provided by other previously used models.	Dutta and Perry (2007)
Studied 4 categories of 2 business lines, and 2 event types of a large financial institution	Developed a matrix: each cell is calibrated by two truncated distributions functions.	Active management techniques would result in significant savings for the bank.	Chapelle *et al.*
Comprehensive look at technical issues of implementing LDA	Loss Distribution Approach	Confidence intervals are useful tools to address the capital estimation.	Frachot *et al.* (2001)

Chapter IV

4. Operational Permanent Control Project

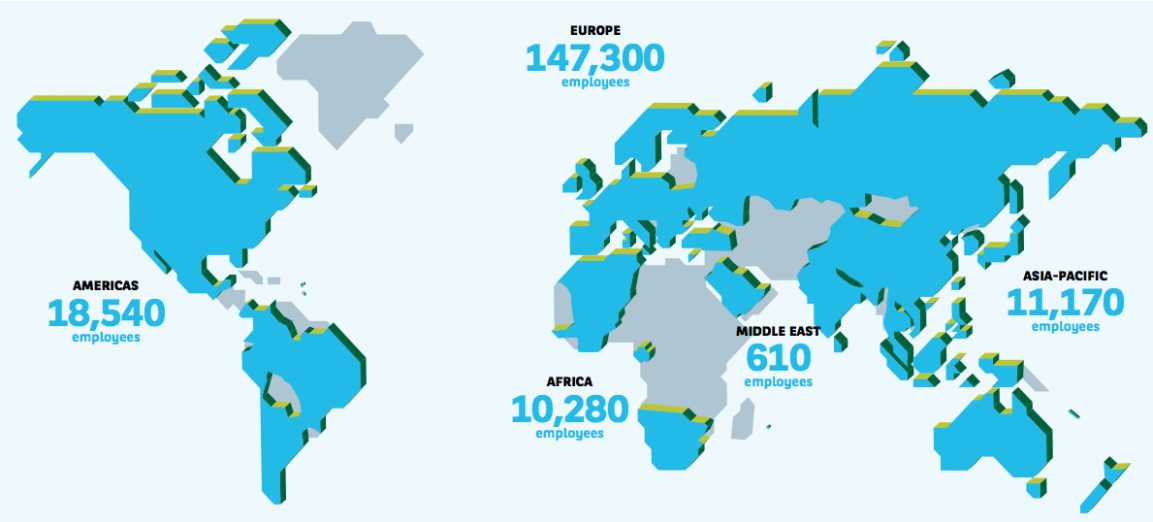
In this chapter, we introduce the corporate profile and global organizational structure of BNP Paribas, globally, as well as in Portugal. We dive deeper into the organizational structure by specifically describing the Department, team in which the Traineeship falls under, as well as the Traineeship role itself. Thereafter, we discuss the process of developing theoretical risk maps and controls as it pertains to hypothetical teams at BNP Paribas Lisbon. Subsequently, we explain in detail the procedures that creating a control model for Front Officers entails. Lastly, we discuss notorious financial cataclysmic events that could have been mitigated or completely avoided through an efficient operational risk management system.

4.1 Corporate Profile: About BNP PARIBAS

BNP Paribas is a large French multinational bank and financial services provider that offers a range of banking and financial solutions serving the needs of individuals, and commercial, corporate and institutional clients. Though the bank has its headquarters in Paris, it has a global footprint, with banks, service centers, and operations in seventy-five countries across Europe, the Middle East, Africa, the Americas, and the Asia-Pacific.

BNP Paribas Group has more than 189,000 employees, with more than half based in the bank's four European 'domestic' markets: Belgium, France, Italy and Luxembourg (BNP Paribas, 2015). BNP Paribas is a leader in banking and financial services in Europe. Since it is one of the biggest banking groups across the world, it has a high brand visibility. It has cultivated a strong brand name and reputation, which in turn facilitated its good financial positioning.

Figure 3: Map of BNP Paribas' Global Operations



Source: BNP Paribas Annual Report (2014)

4.1.2 BNP Paribas in Portugal

Since 1985, BNP Paribas has been the sole operating French bank branch in Portugal and its one of the biggest foreign organizations in the country. It functions through nine affiliates and branches and covers the Group's two main businesses: Corporate and Institutional Banking, and International Retail Banking & Services. These two core activities are complementary and provide a strong foundation for BNP's strategy and assure financial robustness.

BNP Paribas Portugal provides services to the corporate and institutional clients ranging in diverse areas: capital markets, structured finance, commercial banking, asset management, securities services, leasing, factoring, account services and vehicle management services. Moreover, the bank offers financial services to different group entities locally and internationally; in Portugal particularly, the bank is principally positioned to service big companies, multinationals, financial organizations and institutional investors.

4.1.3 Traineeship Organization

Within the two core activities, Retail Banking and Services and Corporate and Institutional Banking (CIB), the traineeship belongs to CIB. BNP Paribas' CIB operates in 45 countries, has almost 20,000 employees, and is in the forefront of investment banking in Europe (BNP Paribas, 2015). CIB offers financing, advisory and capital markets services and is split into three business lines: BNP Paribas Securities Services, Corporate Banking, and Global Markets (BNP Paribas, 2015). The traineeship falls under the Global Markets OPC & TAC Coordination team.

4.1.4 Department Overview

CIB offers capital market business through its Global Markets department, which provides solutions across asset classes, and industry-leading services for clients including Institutional, corporates, private banks and retail distribution networks. Global Markets is comprised of seven global business lines; G10 Rates, Equity Derivatives, Forex & Local Markets, Commodity Derivatives, Credit, Prime Solutions & Financing and Primary Markets.

The Global Markets department aims to serve their franchise of clients though exposing efficient ways to raise and invest capital as well as manage their exposure to risk. Global Markets employs over 3,700 staff globally throughout Europe, Middle East, Africa, the Americas and Asia Pacific. With the main trading floors located in London, Hong Kong, New York, Paris, Singapore and Tokyo.

4.1.5 Operational Permanent Control Process Overview

The Global Markets Operational Permanent Control, OPC from here on, team ensures that all processes comply with CIB methodologies, tools and standards, as well as are in accordance with specific market regulations. There are several missions that the team

handles that could be split into four areas: Validation Process, Risk reduction, Control Plans, and Governance and Reporting.

The OPC team ensures that validation process complies with the CIB practice and supports the Committee Chairman. Under this process, the team performs operational risk assessment encountered by any new activity. Thus, the team should coordinate the approval policies under the business responsibility and ensure that all processes, transactions, strategies, etc., adhere to it.

Debatably the biggest area the OPC team is concerned with is risk reduction. Reducing the risk profile entails monitoring and analyzing historical incidents and the related action plans. In addition to the historical incidents, it is important to create and maintain a record of potential incidents. The team should monitor and follow-up recommendations from internal and external audits that expose certain business vulnerabilities. In order to implement an adequate control plan, the team must perform risk assessment according to the processes, risks, and controls approach and, ultimately, develop the operational risk cartography.

The OPC team is in charge of designing, building, implementing and continually improving the control plans. The control plans should be cohesive for all business lines and regions and must obey the practices, policies, guidelines, etc. The team must also ensure that there are tools in place to ensure materialization of the controls, related indicators and the possibility to escalate issues relating to the controls. Following the implementation of the controls, the OPC team needs to supervise, monitor and report the deployment of the controls, and ensure a constant progression of adherence to them. The OPC team should consistently look to strengthen the control set up through the implementation of risk reduction actions and solutions. Additionally, in order to reinforce the internal control set up, all projects, regulatory or internally driven, need to have a provision of advisory and coordination established by the OPC team.

Following the controls, the OPC team needs to set up and run efficient governance and reporting systems. The governance on both a global and regional level should be developed through reports or dashboards, and regular meetings with Front Officers, Internal Control Committees, Business Partners and the list goes on.

4.1.6 OPC Analyst Trainee Overview

As an OPC Analyst Trainee, the goal was to ensure that both Operational Risk and Permanent Controls areas completely met their objectives and requirements in an efficient, precise and timely manner. The processes entailed:

- Providing analysis and reports by performing data extraction and updating, analyzing, manipulating, reporting and formatting;
- Collecting and analyzing data, as well as structuring queries and performing routine maintenance of reports;
- Developing special reporting templates to develop new reports;
- Ensuring data input and chasing those responsible to update the data;
- Producing reports in an efficient and timely manner;
- Provide analysis on process, risk review and risk reduction programs.

In addition to these processes, we were responsible for developing and implementing relevant risk cartography and an adequate control plan for the Global Markets Lisbon Front Office team. The following section will delve deeper into the process of building, executing and completing this project.

4.2 Operational Risk Management

OPC, a first line of defense, must be developed in order to properly manage operational risk. The role of the OPC is to develop and implement the operational risk and permanent control management structure. Thus, OPC would go through the process of identifying, evaluating and measuring the risks and then developing procedures and controls to contain these risks.

The OPC team should separate an operational risk incident by the cause, the event, and the effect. The ability to reduce the frequency of an incident occurring and the severity

of its impact when it occurs, or even preventing an incident from occurring all together originates from understanding and managing the causes of previous and potential events. By identifying where the causes are located within vital activities allows the team to take fitting corrective actions. Subsequently, analyzing the development of previous and potential events enables the operational risk management in that it provides clues that will allow the team to anticipate potential events or recognize warning signs that reveal an inadequate or defective procedure. Lastly, the effects are the consequences of the event occurring, typically represented in a financial impact to the entity. By monitoring and reporting incidents, it becomes easier to see if the objective of the operational risk management is being met, which is to reduce the effects of the unfavorable events.

Operational risk management is a precise risk reduction scheme that must be defined in such a way that prioritizes the avoidance, mitigation or transference of the most undesirable risks. There are certain risks that an entity may decide to tolerate due to factors such as lower financial impact and those should also be predefined within a risk mapping scheme.

4.2.1 Operational Risk Cartography

The goal of mapping operational risk is to identify the focal areas of core risks the entity is exposed to, as well as evaluating the residual risk, once the actual permanent control framework and dynamic risk indicators have been taken into account (BCBS, 2003). Risk mapping is an organizational framework that facilitates a systematic approach, with some standardized components, to detecting and measuring operational risks (BCBS, 2003). Once identified and assessed, risk mapping also ensures that the risks produced by daily work activities are formalized and disclosed in a transparent manner. Furthermore, risk mapping helps the entity to identify opportunities where it can take counteractive actions to rectify any potential weaknesses.

In order for risk mapping to be effective, it must first swiftly provide an all-encompassing assessment of the central areas of risks posed to the company. Thereafter, a methodical approach to controlling these risks and a way to evaluate the efficacy of the

approach should be implemented. Risk mapping should also be equipped with robust and adaptive follow up indicators customized for the specific risks involved. Lastly, an exhaustive risk mapping system would emphasize key areas of improvement through providing and consolidating essential information that allows for faster detection.

4.2.2 Controls

A control is designed to increase the likelihood of reaching a predetermined objective while simultaneously managing the risks surrounding the main tasks that must be performed in order to achieve those objectives (BCBS, 2003). By establishing controls that a Front Officers would validate or reject creates a line of communication that facilitates detecting vulnerabilities more efficiently. This validation can be done prior to the execution of the operation or process, which is designed to evade a particular risk or incident, or it can be carried out afterwards, in order to abridge or circumvent completely the impact of an incident.

In order for controls to be effective, there must be a formalized set of procedures. The procedure for controls would specify not only its goal but also why it is relevant to the particular processes. Controls should also have a management follow-up system that would enable managers to identify ways to reduce the detected risks (Chorafas, 2004). Therefore, a control plan is a group of controls that are customized to the specific team's or front officer's main processes and risks.

4.2.3 Risks and controls

An effective control prevents the potential risks or curbs their impact through early detection (BCBS, 2003). The control does not necessarily have to protect against operational risk, it can include various other risks such as credit risk, market risk, and liquidity risk, to name a few.

In order to create an effective control, there must first be an analysis of measuring the risks that the organization is exposed to (Scandizzo, 2005). The intensity of the control

should be consistent with the level of risk and with the organization's risk tolerance (BCBS, 2003). Thus, the greater the risk, the higher the intensity of the control should be. The intensity could be set in various different ways. For example, if an operation or procedure has an intrinsic risk that is low, the frequency of the control can be low and solely the person performing the action can be set to validate it. However, the higher the risk and its potential impact, the more controls are needed that supersede a simple self-control, and may even involve other players, such as the management or a dedicated team, considered a first level control, and/or independent permanent control functions, which would be second level controls.

When assessing the risks involved, there should be a spectrum or a certain mapping that would place the risks by the level of impact that it could potentially have on the entity from lowest to highest. If the risk could have a substantial impact on the assets, reputation or results of the organization, it would be considered a major risk, and the control covering it would also be considered essential. Thus, controls would also be ranked on a scale proportionate to the evaluation of the corresponding fundamental risks.

Ultimately, the systematic analysis of the controls identified follow a risk mapping, but it also needs to be congruous with the AMA approach and the quantified potential incidents in each entity. When taking all the entities as one, there are several processes that inherently expose banks to particular risks. For example, if people miss a particular training, the exposure to human error would, in theory, increase. Thus, there are certain generic controls that would pertain to all departments and people. Therefore, most Business Units should have control plans that would have a set of both, generic controls and customized controls, founded on the assessed risks and the subsequent mapping, and match the units risk tolerance level.

4.3 Project Process

In order to prepare the most effective controls, we scheduled meetings with every team so that they could explain their procedures on a deeper and more detailed level. In this way, we could obtain a comprehensive understanding of the processes that they are

performing and recognize the potential operational risks that they posed to the bank. Once we analysed and the potential risks were mapped, we developed internal controls with the goal of mitigating or possibly eliminating these risks.

The following process descriptions and controls are generic examples of hypothetical teams, which at the time of writing did not exist at BNP Paribas in Lisbon. The examples are intended solely for illustrative purposes and do not reflect or have any connection to the actual processes or controls performed by any team at BNP Paribas in Lisbon.

4.3.1 The Hypothetical Trading Team

In the equity market, market makers would provide different prices on a product depending on their position, meaning whether they are long, in that they are offering to buy the product, or short, which is if they are selling the product. This hypothetical market making trading team offers a range of standardized products to both retail and institutional clients daily with the goal of offering competitive prices. When providing a new product, the trader develops a defined strategy that takes into consideration certain factors such as the margins, payoff, entry and exit points, duration of trade, the underlying, the quantities, hedging criteria, and the list goes on. Once the strategy has been defined, the trader must set specific parameters, which is specific to the product being issued.

Table 3: Control on Pricing and Parameterizations

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on Pricing and Parameterizations	Daily	Mispricing	This control would potentially ensure that the trader has considered the necessary criteria in order to set the appropriate price and the relevant parameters for that particular product.

The frequency of the control depends on the process, since in this scenario products are offered on a daily basis; the risk of a potential mispricing is daily. Thus, this control holds the trader accountable for ensuring that he or she has set the correct price on a daily basis.

Traders must also be aware of events that could have an impact on the product that they are issuing, such as geopolitical events, macroeconomic figures, and corporate actions. Corporate actions are particularly important since it would undoubtedly directly affect the securities issued by that particular company. The objective is to reduce a potential price jump; therefore the objective is to have the price before a corporate action be more or less the same price after the corporate action. There should not be any mispricings that could potentially impact the product that an investor is holding. This requires some calculations and simulations on the trader's part, in order to predict how the product will be and how its barrier, parity, volatility, etc. will change.

Table 4: Control on potentially impactful events and corporate actions

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on potentially impactful events and corporate actions	Weekly/Monthly	Follow up Failure, Mispricing,	This control would potentially ensure that the trader has closely monitored events that could cause a mispricing or give rise to an arbitrage opportunity. Therefore, the trader must take the measures necessary by either making adjustments or even removing the product from the market to avoid the potential of a price jump.

Since potentially impactful events do not happen on a daily basis, this control monitors whether the traders are following up on a weekly or monthly basis. The risk of not following up could result in a financial impact on the desk from that trade.

A trader must have knowledge of the financial impacts that each trade can have, whether positive or negative, and he should always have an exit strategy before even

entering the position. Otherwise, the losses incurred from any particular trade could be insurmountable and catastrophic. The risk would be a Misexecution, in that the trader has poorly executed the trade and its strategy by not implementing a Stop Loss Order.

Table 5: Control on Stop Loss Order

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on Stop Loss Order Strategy	Daily	Misexecution	This control would potentially certify that the trader has established an order that would immediately close the position should the trade go in a losing direction.

It goes without saying that traders should operate under the rules of the market and the regulations, however risk control measures are needed to help ensure ad monitor that these rules are respected. In order to prevent rogue trading from going undetected, many investment banks have increased their monitoring and set up certain controls. One example is having a minimum period that the trader should be away on vacation so that any suspicious activity would be uncovered during that time. The following are several controls that any investment bank should have in order to reduce the probability of rogue trading from occurring.

Table 6: Control Plan Example List

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on risk limits and exposure	Daily	Poor position oversight	This control would theoretically safeguard the bank from a particular level of risk exposure. Thus, this control would ascertain that the trader has not surpassed the market risk limits that have been predetermined.
Control on Profit and Loss Reconciliation	Weekly	Failure in Reconciliation	This control would hypothetically make sure that the last Profit and Losses reported by the Middle office matches the trader's calculations. Any discrepancies would be analysed and explained or fixed.
Control on market rules, regulations, and compliance	Monthly	Breach of market rules and regulations	This control would potentially guarantee that the trader has obeyed market rules, regulations, and compliance in each of the trades performed.
Control on minimum holiday period	Annually	Internal Fraud	This control would ideally enforce a block leave period for its traders in order to help the bank detect if any fraud or rogue trading is occurring.

Traders must have a predetermined risk limit that they must stay within when performing each trade, if not respected they risk exposing the bank to more risk than the bank intended. Additionally, a trader's profits and losses should not only be monitored, but also reported on a constant basis. This is not only to ensure at the trader is not hiding a substantial amount of losses, but also to raise a red flag of a potential rogue trader. Thus, the amount that the trader reports should match the amount stated by the middle office, however if it does not then the necessary adjustments should be made.

Ultimately, the goal is to mitigate or prevent potential operational risk that all of the teams pose with their day to day processes. These descriptive controls represent the type of customized controls that we developed for each team, once we analysed the type of risk that each process contained.

4.3.2 The Hypothetical Structuring Team

The structuring team develops customized products to address the different needs of a wide range of clients, which can entail financial institutions, retail and corporate clients, to even governments. A structured product is a tailored investment strategy composed of derivatives, such as securities, options, commodities, currencies, etc. A structurer must not only be concerned with developing products that meet the complex needs of the clients but that also satisfy the needs of the bank.

Since structurers are dealing with non-standardized products, it is imperative that they understand how to appropriately price the products created that can handle volatility and different market environments.

Table 7: Control on Pricing

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on Pricing	Daily	Mispricing	This control would potentially ensure that the structurer has considered the necessary quantitative models and criteria in order to set the appropriate price for the specific products.

Different products will be at different stages of execution, thus a structurers concern would not solely be pricing. There would also be products that would have closed, and in order to ensure that the financial needs of the clients are being met, the structurer should review the performance of that product and work to adapt future products to consistently improve the products being created.

Table 8: Control on closed product follow up

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on closed product follow up	Weekly	Follow up failure	This control would potentially ensure that the structurer has reviewed the performance of the product and has made the necessary adaptations.

Although the regulatory framework for non-standardized products can be unclear due to products falling within legal grey areas, a structure must be mindful of the potential regulatory breaches and avoid them when creating new products.

Table 9: Control on abiding regulations

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on abiding regulations	Monthly	Breach of market rules and regulations and Legal Issues	This control would potentially ensure that the structurer has taken into account the pertinent regulations and has ensured that the customized product does not in any way potentially breach market regulations.

4.3.3 The Hypothetical Marketing Team

The marketing team in an investment bank prepares the advertising material of the standardized products offered to investors worldwide by the bank. When developing new marketing material, the marketing team must ensure that the material is ethical, in that it does not mislead investors in any particular way. The material should also be accompanied with the appropriate disclaimers to circumvent any potential consumer loss of confidence in the financial system. This is to avoid any misleading adverts that could promote false

financial information and lead to investor loss, which would severely damage a client's relationship with the bank.

The hypothetical marketing team's goal is to entice the client to do business with the bank through an accurate portrayal of the range of standardized products that the bank offers with honest financial promotion.

Table 10: Control Plan on Marketing Material

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on Marketing Information Rules and Consumer Confidence	Daily	Breach of marketing regulation rules	This control would potentially ensure that the marketing team has taken the appropriate measures to safeguard consumer confidence by placing the appropriate financial information in its marketing material as well as the relevant disclaimers.
Control on material accuracy	Daily	Misleading Marketing Information	This control would have the marketing team confirm that the information stated in the documents is, to the best of their knowledge, reliable, accurate, viable and relevant.

The frequency of the control, in this instance, would be daily since the team should be concerned with accurate and updated information on all its marketing material. The risk of not following legal or regulatory requirements or product literature that is incomplete or outdated should be a constant concern for the marketing team as not complying could potentially result in a fine or lawsuit.

Information is key in the investment world and it is of great importance that the marketing team treats the sensitive information that it has with the appropriate caution.

Thus, it is of imperative that they always ensure that the appropriate information reaches the relevant people.

Table 11: Control on releasing the appropriate information

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on releasing the appropriate information to the relevant people	Daily	Miscommunication	This control would ideally ensure that the marketing team sends the right information to the appropriate person.

Therefore, the aforementioned control would be to ensure that the team takes the necessary measures to protect and deliver the necessary information to the relevant people. Since the marketing team communicates information on a daily basis, the frequency of this control would also be daily.

4.3.4 Hypothetical Sales Team

The sales team works in collaboration with the traders, structurers, marketing team to help meet the clients' financial needs. Similar to the marketing team, the sales team should be weary of not giving wrong information or the right information to the wrong client. This would also be in regards to the types of arrangements and products that the sales team organizes with the clients, ensuring that it would also be feasible for the traders and the structurers to accomplish.

Table 12: Control on external communications

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on external communications	Weekly/Monthly	Miscommunication	This control would potentially ensure that the sales team has taken into account the pertinent information that they will reveal and the agreements that they would make.

The sales team in particular forms part of the representation of the bank that it is performing business for. Therefore, the sales team poses a reputational risk to the bank and should always ensure that all of their interactions fall in line with the bank's policy.

Table 13: Control on ethical product selling

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on ethical product selling	Daily	Reputational Risk	This control would ideally ensure that the all of its sales interactions are professional, ethical and done according to bank policy.

One control that has not been previously mentioned but would be pertinent for all the teams is an operational risk control escalation. This control would ensure that if an adverse event occurs that does not fall within the scope of the other controls, that the Front Officers still have a way of reporting these issues. Thus, this would be one of the several common controls that would form part of all officers performing tasks.

Table 14: Control on operational risk escalation

Control Plan	Frequency	Risk Involved	Objective of the Control Plan
Control on operational risk escalation	Daily	Operational Risk	This control would ideally ensure that the any operational risk has been appropriately informed and escalated even if it did not fall within the scope of the other controls.

4.4 Creating the Control Model

Once the risk mapping and control plan has been established, the team can now design the control model in ARIS. ARIS is a tool that facilitates the creation of the organizational structure, as well as the controls to manage the processes. The utilization of this tool follows several rules and steps, which will be described further in the following sections.

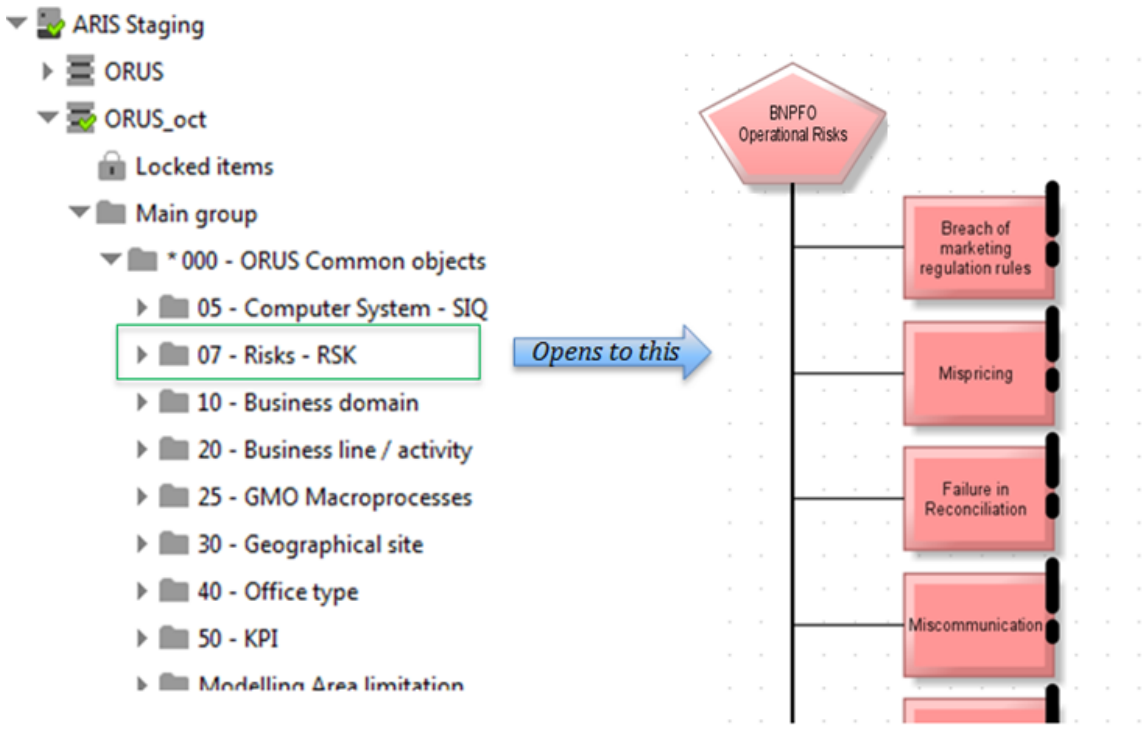
4.4.1 ARIS Business Designer Modelization

ARIS Business Designer, referred to as ABD from here on out, is a tool used to create, manage, analyze and administer the control plan models for front officers and their organization. There are very specific modeling rules which must be respected when creating scripts and models within ABD, which will be discussed in further detail within this section. Once the modeling is complete in ABD, it is then used to generate the ARCM, also called ORUS FO. ARCM is the website in which the front officers see their controls, can validate them, and, if relevant, mention any operational risks they encountered while performing their processes.

Within ABD there are several different databases, which contain specific projects regarding Back Office, Middle Office and Front Office. There are certain objects that all

projects have in common and they are stored in the "000 – ORUS common objects." In regards to control plans for front officers, we are only concerned with the Risks folder.

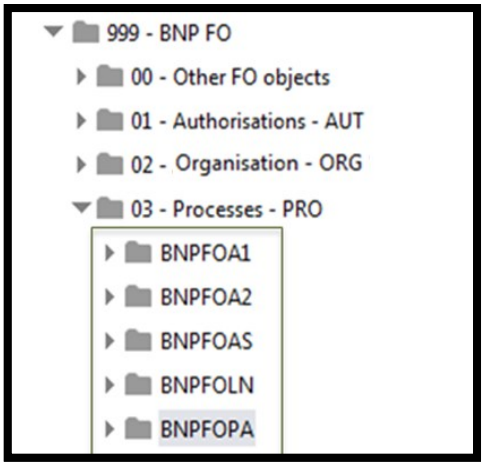
Figure 4: ARIS Risk Mapping



The risks folder is a sort of library that contains all the risks categories developed within the risk mapping process. Thus, the risk folder represents the risk categories that are reduced by the controls developed. Since various controls can reduce the same risk, these objects will have re-occurrences in several models. OPC created this risk cartography, and thus we are in charge of creating or modifying the risk names, if needed.

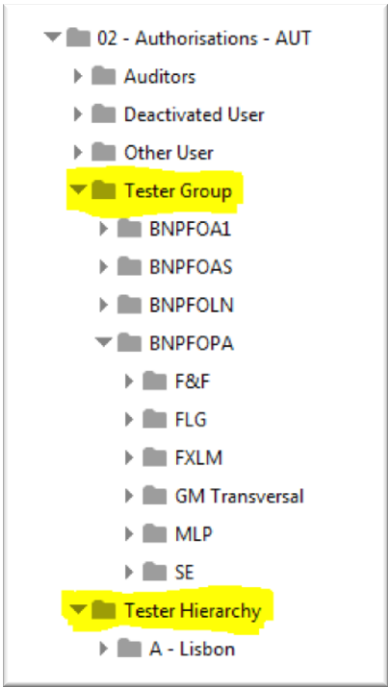
When designing the control plans for front officers for ARCM, the process must be managed and monitored through clients. Clients are classified by the main regions that the front officers are based out of, such as Asia (AS), London (LN), Paris (PA) and the Americas (A1 and A2).

Figure 5: Client Folder list



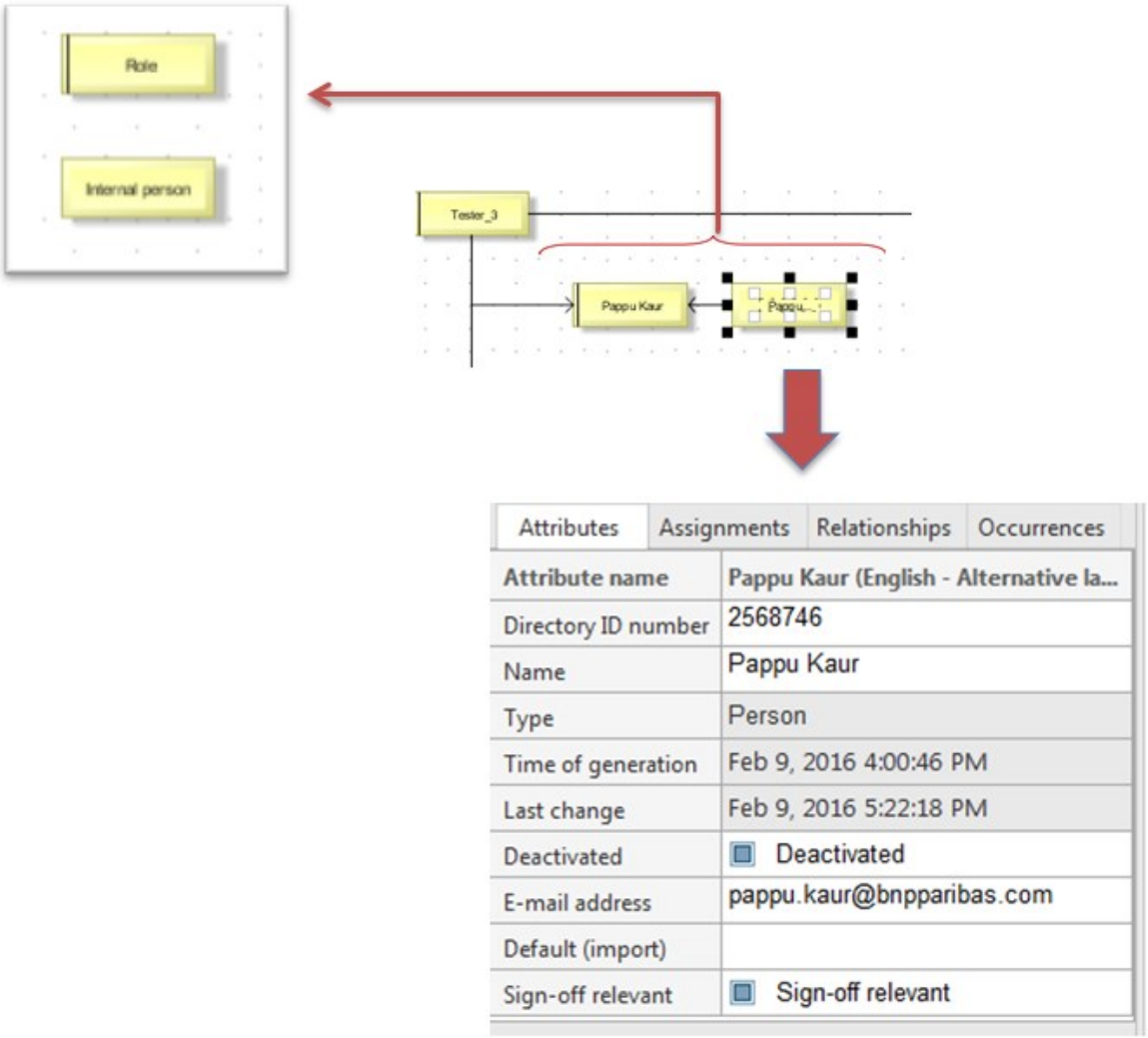
Within the BNP FO folder, there are three main folders that we use: 01- Authorisations, 02 - Organisation and 03- Processes. The Authorizations folder is an organization chart that sets people's identities, access rights along with their teams and managers. Within the folder, there are several models but only two will be discussed as it concerns the creation of teams, those are Tester Group and Tester Hierarchy.

Figure 6: The Authorisations folder



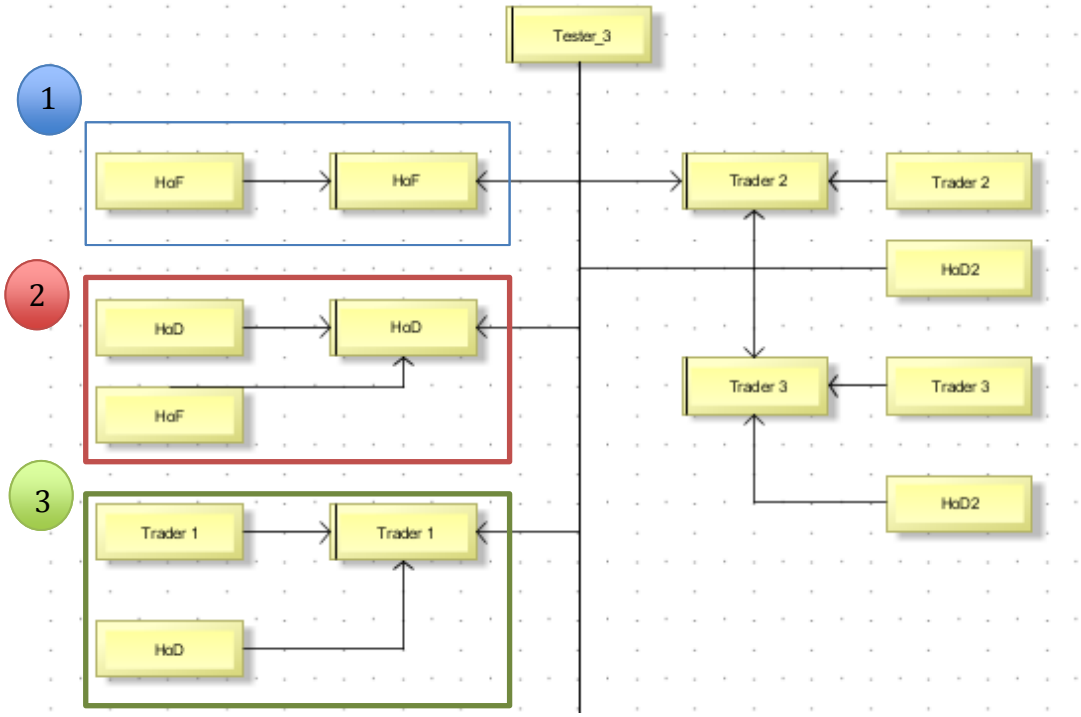
As can be seen in the image above, tester group is separated by client and then within that by business line. The tester group contains the users that actually utilize ORUS and are organized by Role and Internal Person. The Role and the Internal person represent one person, however the internal person contains information such as the ID number and email of the Front officer. The internal person is the user and the Role will connect the internal person to the access rights.

Figure 7: Users' Profile



Each Role will be linked to the tester group, their internal person as well as the internal person of their manager, who will be the one reviewing their controls. As shown in Figure 8:

Figure 8: Hierarchal Tree of Users

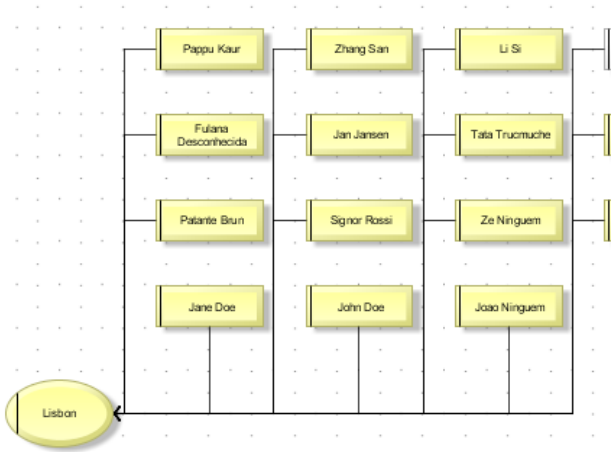


In the hierarchal tree, the Head of Filiere (HoF) is the top manager who reviews the Head of Desk.

- Since the HoF is not reviewed by anyone, only his internal person is connected to the Role, which is then connected to the Tester group.
- The HoF reviews the controls of the HoD, thus Role of the HoD will be linked to two internal persons, its own and the manager.
- The HoD manages the members of his team, and thus his internal person would be attached to the Role of the team member that he oversees. Therefore, the Role should have the same name as the internal person that it represent and will be attached to that member, as well as the manager that will be reviewing the controls.

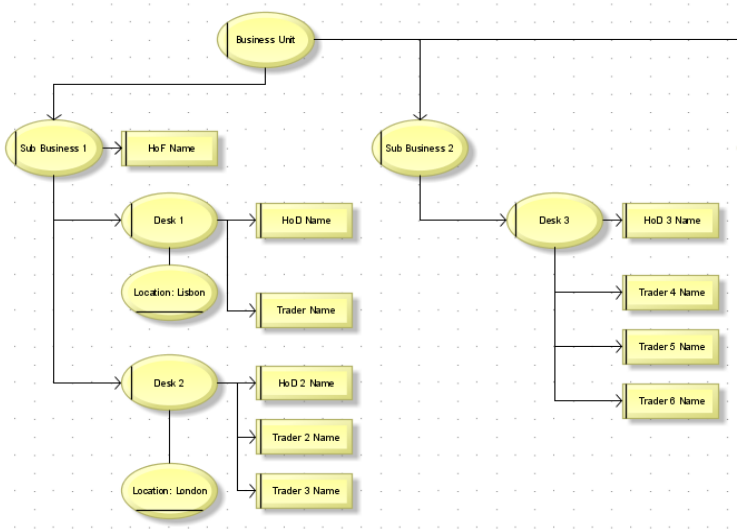
The second folder, within Authorizations, is the Tester Hierarchy which is a technical folder that essentially connects a Role to a hierarchy diagram. This is an organizational diagram that simply reflects the organization for the Front office within one location.

Figure 9: Organization Within a Location



Similar to the Authorisations folder, the Organisation folder also contains an organizational chart but this chart contains each client and is organized by business line. Within the chart the roles of each member are assigned to a team and an organization level.

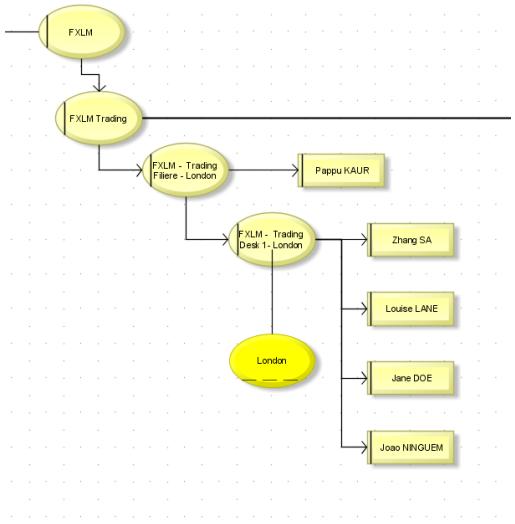
Figure 10: The Organizational Units By Levels



The Organizational units reflect the organization through four organizational levels:

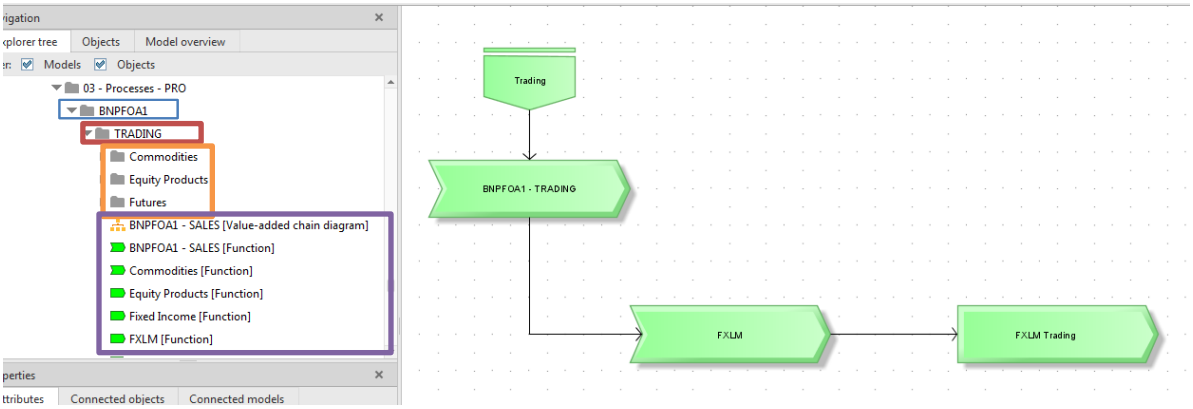
- Business Unit
- Sub-Business Unit
- Filiere
- Desk

Figure 11: FXLM Example of the Organizational Levels



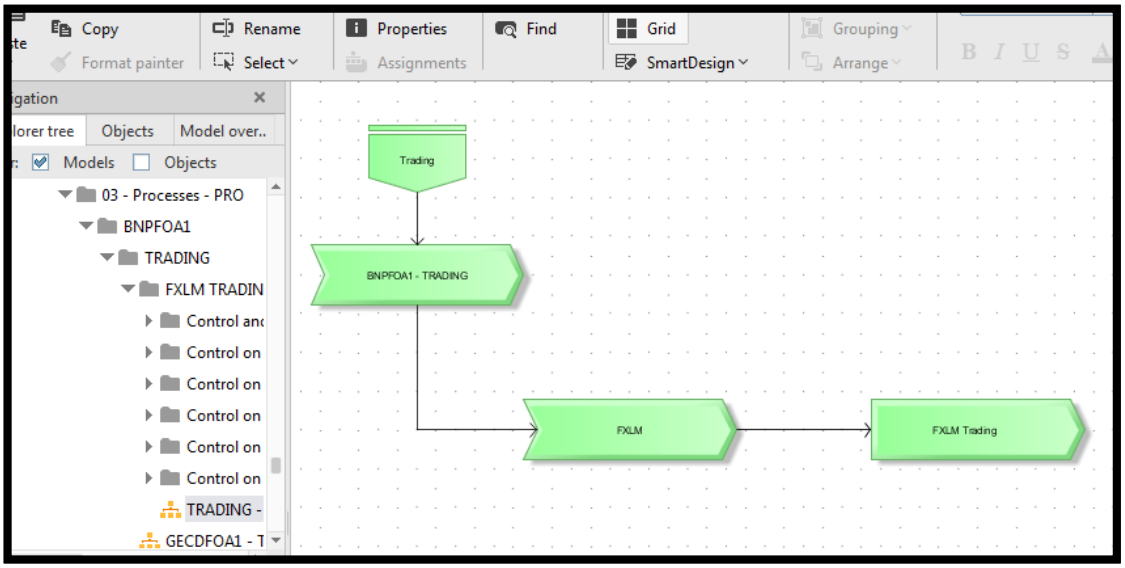
In this example, the Business Unit is Forex and Local Markets (FXLM), there can be several Sub-Business Unit, such as FXLM Marketing, FXLM Sales, FXLM Trading, as portrayed above, etc., that would all connect to the larger Business Unit. Filiere is the third organizational unit and it is comprised of all the desks that fall within that division. The Head of Filiere, in this case Pappu Kaur, would be linked to this division and he would oversee and review the controls for all the HoD's of the desks that fall within that division. Each desk is linked to a location and the HoD, in this instance it is Zhang Sa in London, and the rests of his team members that he will be reviewing are linked thereafter.

Figure 12: The Process Folder



The Process folder is organized by client, such as BNPFOA1, and each client contains a folder with the separate business domains. So within BNFOA1, there could be a folder for Trading, Sales, *etc.*, which can then be further subdivided into Sub Business Units. The business domain will be comprised of the "Value added chain diagram" (VACD) model, which contains Macro-processes and process objects as well as "Business Unit" folders, which contain each process assignments.

Figure 13: The Value Added Chain



As shown in the image above, all value added chain diagrams begin with the Business domain, in this instance it is Trading. Trading is then linked to a profile within the client, in this instance BNPFOA1 – Trading, the first Macroprocesses. The "Business Unit" Macroprocesses, FXLM in this instance, is linked to the first Macroprocesses and is subordinate to the first. The Sub Business Unit, in this case, FXLM Trading, is subordinate to the Business Unit and are assigned a new model called Event Process Chain, or EPC hereinafter.

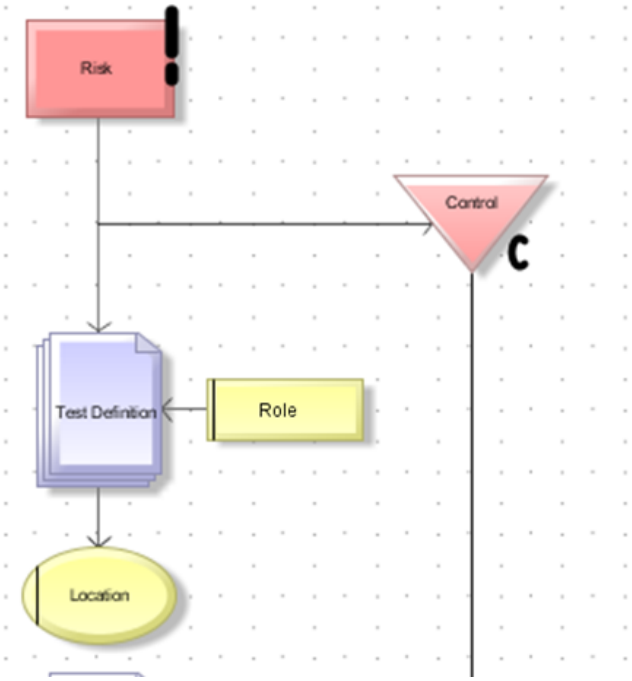
The EPC model is used to sort activities and controls and it is where all control objects are stored. The EPC model linked with the Sub Business Unit process is stored in a specific folder, FXLM Trading as shown in the image above. FXLM Trading, as all other Sub Business Unit folders, contains the control folders that hold the Business Control diagram. Each activity or control object with an active status must be connected to a unique EPC. So there will be one activity per EPC that can be linked to several controls as shown below.

Figure 14: The Event Process Chain

Every “Control” mentioned in this EPC must have an occurrence in a Business Control diagram (BCD) through an assignment that will connect it to a new BCD model, portrayed by the green and red tripod above. The Business control diagram is comprised of the control that is to reduce one specific risk, which is obtained from the aforementioned ORUS Common Objects. Risks are stored in the Risks Folder and copied into the Business Control diagram representing its mitigation through the controls.

Each Control object must be connected to at least one “Test Definition” object, which defines the attributes of the control for that specific user. The Test definition will contain the name of the control, the time of generation, the frequency, and the time limit that the particular FO will have to complete that particular control.

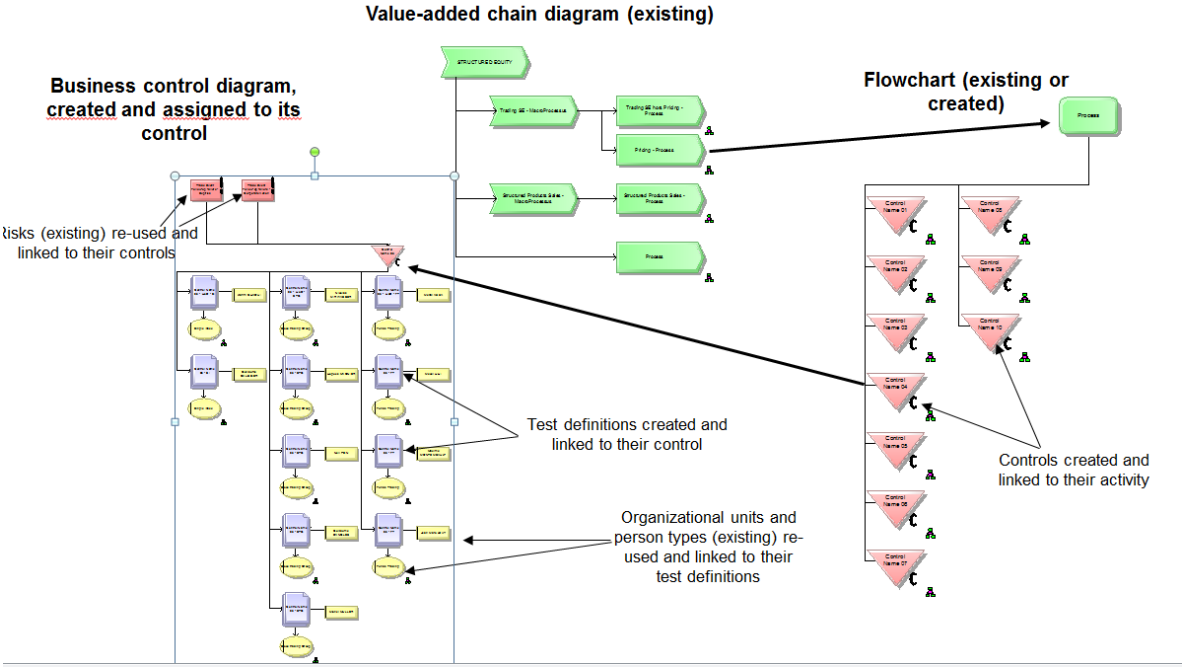
Figure 15: Business Control Diagram



Once all the controls have been created for that specific team it is now ready to be imported into ARIS Risk & Compliance Manager (ARCM).

To summarize, there are two main processes in regards to developing the ARIS Model. There are the organizational aspects, such as the Tester group and tester hierarchy, and the management aspects, such as the VACD, the EPC and the BCD.

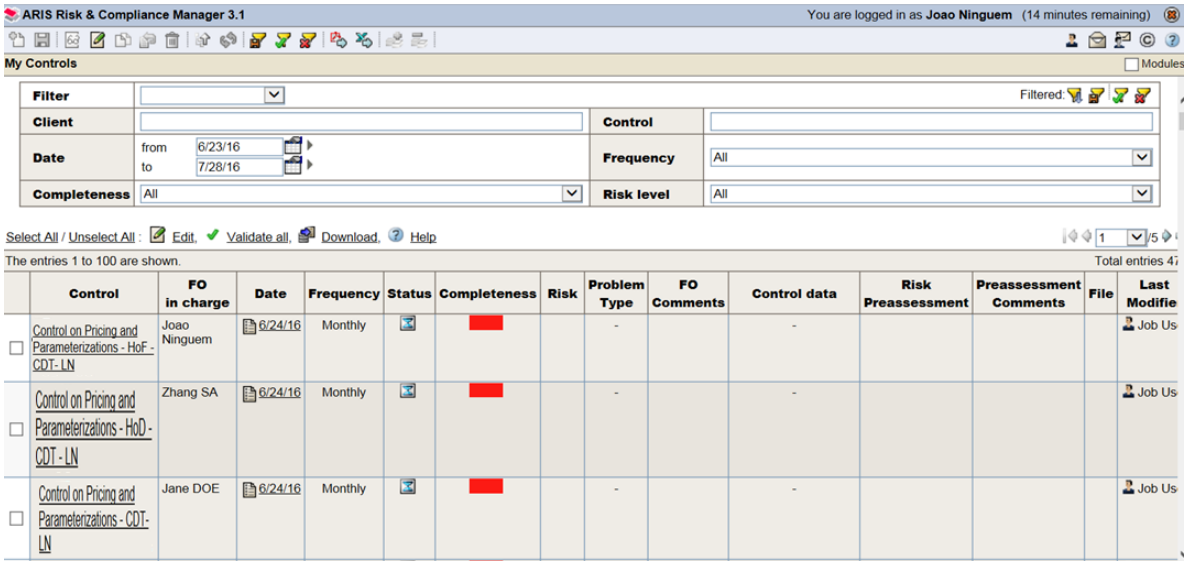
Figure 16: Global View of the ARIS Modelization Process



4.4.2 ARIS Risk & Compliance Manager

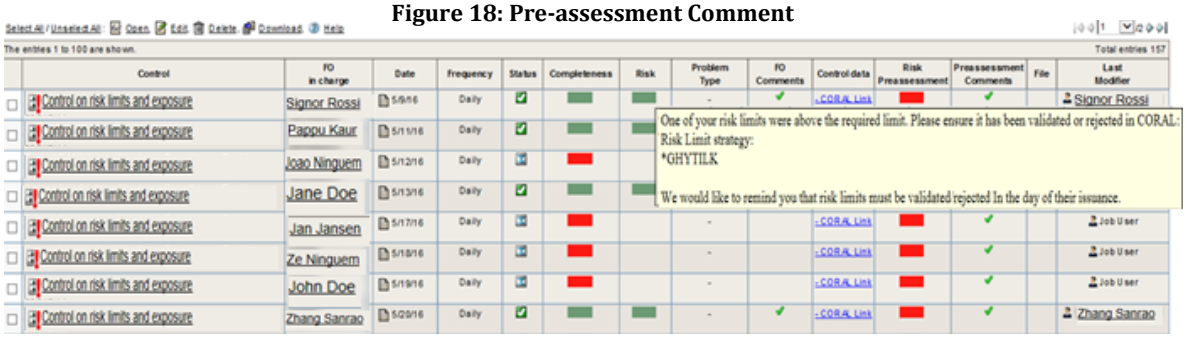
Once the processes have been designed, the process is ready to be introduced and viewed in the ARCM internal website system. ARCM is a safe and shared system that allows Front Officers to see and validate their controls, as well as raise any issues that they may have encountered when performing their processes. Moreover, ARCM offers a two-way interaction between Front Officers and OPC team, since the team can also comment and inform the Front Officer through those controls of any potential vulnerabilities that the OPC team would have spotted.

Figure 17: ARCM Control Plan View



In the figure below, we are observing the access view of Joao Ninguem, who is an HoF. As previously mentioned, an HOF also monitors the control completion of the people within his team, which is why in this scenario he can also see the profile of Zhang SA and Jane Doe. Otherwise, normal Front Officers would only have access view and validation rights to their controls only.

Figure 18: Pre-assessment Comment



The figure above portrays a message that an OPC team member could send to a Front Officer, who is being informed of a process that requires an action as to avoid a risk. The risk Pre-assessment is red to signify that the risk of not performing that particular process is high. Thus, the OPC team has managed to detect a potential risk early and inform the Front Officer involved so that an action to avert this particular risk is taken. Therefore, ARCM is an effective systematic tool of managing, controlling and mitigating the potential risks.

4.5 Hypothetical to Reality

The importance of an efficient operational risk management system truly becomes apparent after actual events occur that prove to be cataclysmic for the financial institutions involved. Many times these events, in hindsight, show that preliminary steps could have been taken to either reduce their impact or completely prevent them from happening. These events highlight the vulnerabilities that financial institutions face by not establishing strong systematic and effective operational risk defense systems.

There have been several high profile operational risk incidents that have proven costly for the financial institutions impacted. Three high profile cases were that of Barings Bank, Société Générale and UBS, each of which separately experienced losses above the billions due to the sole activities of one of their traders. Although these rogue traders were ultimately at the root of these catastrophic events, the actual problem began with the lack of a strong systematic approach to managing operational risk. Within the Basel Committee's definition of operational risk, the risk of loss resulting from people is a risk that banks' need to constantly address (BCBS, 2001).

Through unauthorized speculative trades, trader Nick Leeson amassed losses of over $1 billion USD at Barings Bank, ultimately bankrupting the bank (Hoch *et al*., 2001). However, the lax management structure at Barings Bank also contributed to its own collapse as it had provided an environment in which Nick Leeson could go undetected with his risky transactions until it was too late. Although the Bank of England acknowledged Nick Leeson as the only culprit of the fraud, it stated that there also existed a "serious failure of controls and managerial confusion within Barings" (Hoch *et al*., 2001).

In similar cases, Jérôme Kerviel and Kweku Adoboli also conducted unauthorized trades that cost their respective banks, Société Générale and UBS, billions. In 2008, Jérôme Kerviel had incurred a 4.9 billion Euro loss at Société Générale from duplicitous trading transactions (Gilligan, 2011). Three years later, UBS found itself in a similar situation having declared losses of $2.3 billion USD suffered from the deceitful synthetic equity trades of Kweku Adoboli (Gilligan, 2011). However, these are not isolated incidents, since the collapse of Barings Bank in 1995 there have been several prominent cases of rogue trading incidents that have led to financial institutions incurring losses into the billions.

However, operational risk does not necessarily solely occur with one single perpetrator. There are instances in which misconduct can occur at a bigger scale that leads to an environment in which it is embedded on a day-to-day basis. The London Interbank Offered Rate (LIBOR) manipulation scandal is one example of fraudulent actions that occurred on a mass scale and relied on nonexistent or weak operational risk management systems. The LIBOR is a group of rates established by a "panel" of "contributor banks" that represent the borrowing rates of ten different currencies (McConnell, 2013). The LIBOR fixing process relied on the "trust" and impartial opinion of these experts, however what occurred instead was a manipulation of the LIBOR rates that benefitted particular individuals and firms to the detriment of borrowers around the world (McConnell, 2013). The LIBOR rates scandal was not an isolated even but a systematic widespread "business-as-usual" manipulation that involved many managers and traders from different organizations (McConnell, 2013).

One major operational risk vulnerabilities that the LIBOR rates process possessed was that the oversight and sanctions were regulated by the contributing banks themselves (McConnell, 2013). In other words, there was a lack of management systems that were judicious, transparent and ensured an ethical estimation of the rates. Furthermore, it seems that several entities and individuals within and outside of the "panel" were aware to some degree that the LIBOR process contained misleading or inaccurate reports (McConnell, 2013). This indicates a lack of accountability in regards to reporting potential misconduct occurring amongst the experts. The manipulation was found to be a nearly quotidian occurrence involving multiple traders, submitters of rates, and managers (McConnell, 2013). Furthermore, it was found that some rate submitters were also derivatives traders themselves who based their submissions on their own desk's trading positions (McConnell, 2013).

Ultimately, these cases illustrate the impact that an inefficient or nonexistent operational risk management system could have on a financial institution. They emphasize the importance of implementing operational risk management systems that would potentially protect financial institutions, and ultimately the financial markets, from being negatively impacted by operational risk that can result in catastrophic events.

Chapter V

5. Conclusion

Notable operational risk incidents, such as those of rogue traders Nick Leeson at Barings Bank, Jérôme Kerviel at Société Générale, and Kweku Adoboli at UBS, highlight the potential consequences of not establishing strong and efficient operational risk management systems. Each of these aforementioned traders caused their banks billions due to unauthorized transactions that they undertook, and in the case of Nick Leeson led to the collapse of the bank (Gilligan, 2011). In hindsight, had these unauthorized transactions been caught earlier the financial impact could have been much smaller and possibly insignificant. Therefore, these incidents also highlight that there existed standardized and structural drivers within the environment of these financial institutions that allowed for these events to occur and thus ultimately contributed to their own demise.

However, misconduct does not solely occur as isolated events from one individual at a financial firm. As the LIBOR scandal illustrated, the origins may begin small but can escalate into a large global systematic way of conducting business. Thus, efficient operational risk management systems are crucial not only to helping financial institutions curve the potential impacts that they face from operational risk but also to prevent these impacts from negatively spilling over into the financial markets.

Ultimately, establishing a methodical and effective first line of defense is crucial for detecting potential risks as early as possible and, consequently, mitigating or completely avoiding the impact of those risks on the financial institution. Therefore, financial institutions must take defensive measures against potential risks in order to protect their financial, reputational, and/or operational stability from being negatively affected by unfavorable, unforeseeable events.

In this study, we performed an internal analysis of the processes performed by the BNP Paribas Global Markets Front Office team in Lisbon in order to deduce if there was, in fact, a need for an operational risk management framework. We found that it was helpful and necessary to implement operational risk management frameworks. Therefore, we developed risk cartography as it pertained to the processes performed in Lisbon and,

subsequently, internal control systems with the objective of combating these identified risks. Although a complete risk-free environment does not exist, financial institutions should have the objective of reducing the occurrence and/or impact of these risks through strong operational risk management systems, which we achieved through the development and implementation of a tailored and comprehensive operational risk management model.

This study has meaningful contributions to the literature since, to the best of our knowledge, it is the first case study performed on BNP Paribas Lisbon in regards to operational risk. We also deduced that this is the first study to simultaneously discuss the development of risk cartography and the implementation of a risk control system through ARIS. Furthermore, the study contributed to the operations of the BNP Paribas Lisbon office through the analysis and implementation of enhanced risk controls, which could ultimately help in limiting any potential impact of risks that could occur.

The main limitation of this research was the sensitivity of the information that, because of confidentiality reasons, could not be used to further the study. It would have further enriched the study if we could have been able to use internal data. It would be interesting to see future research that delves into the quantitative aspects of operational risk management using the internal data of a bank.

Furthermore, the Basel II Accord will soon be obsolete as banks begin to implement the Basel III Accord, thus, it would be intriguing if the subsequent research highlights the impact this new Accord will have in regards to the qualitative, as well as the quantitative aspects of guarding against operational risk.

References

Alexander, C. (2003), *Operational Risk: Regulation, Analysis and Management*. London: Financial Times Prentice Hall. Print.

Balin, B. J. (2008), "Basel I, Basel II, and Emerging Markets: A Nontechnical Analysis." Social Science Research Network. N.p. Web. 12 Mar. 2016.

Basel Committee on Banking Supervision (2001), *Consultative Document: Operational Risk*, Available at http://www.bis.org/publ/bcbsca07.pdf, accessed on 27 July 2016

Basel Committee on Banking Supervision (2003), Sound Practices for the Management and Supervision of Operational Risk, Available at http://www.bis.org/publ/bcbs96.pdf, accessed on 22 August 2016.

Basel Committee on Banking Supervision (2011), Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, Available at http://www.bis.org/publ/bcbs196.pdf, accessed on 27 July 2016.

Basel Committee on Banking Supervision (2015), *A brief history of the Basel Committee*, Available at http://www.bis.org/bcbs/history.pdf, accessed on 27 July 2016.

BNP Paribas (2014), *Annual Report 2014*. Retrieved from https://invest.bnpparibas.com/sites/default/files/documents/bnp_paribas_ra_2014_en_02.pdf, accessed on 24 April 2016.

BNP Paribas (2015), *Annual Report 2015*. Retrieved from https://invest.bnpparibas.com/sites/default/files/documents/bnp-ra2015-va_e-accessible.pdf, accessed on 22 April 2016.

Chorafas, D. N. (2004), *Operational Risk Control with Basel II Basic Principles and Capital Requirements.* Amsterdam: Butterworth-Heinemann. Print.

Dutta, K. and J. Perry (2007), A Tail of Tails: An Empirical Analysis of Loss Distribution Models for Estimating Operational Risk Capital, Federal Reserve Bank of Boston, Working Paper No 06-13. Available at http://www.bos.frb.org/, accessed on 12 March 2016

Engelen, E. (2011), "Banks Misunderstood." *After the Great Complacence: Financial Crisis and the Politics of Reform*. Oxford: Oxford UP, pp 97-131. Print.

Ferrell, O. C., J. Fraedrich, and L. Ferrell (2010), *Business Ethics: Ethical Decision Making and Cases: 2009 Update*. Mason, OH: South-Western Cengage Learning. Print.

Frachot, A., P. Georges, and T. Roncalli (2001), Loss distribution approach for operational risk. *Available at http://www.mathsfi.com/malliavin/Loss_Distribution_ Approach_in_Practice_05_02_2003.pdf*, accessed on 12 July 2016.

Gilligan, G. (2011), Jérôme Kerviel the 'Rogue Trader' of Société Générale: Bad Luck, Bad Apple, Bad Tree or Bad Orchard?. The Company Lawyer, Vol. 32, No. 12, pp. 355-362, 2011. Available at SSRN: http://ssrn.com/abstract=2014487, accessed on 29 Auguat 2016.

Hoch, S. J., H. Kunreuther, and R. E. Gunther (2001), "Chapter 1: A Complex Web of Decisions." Wharton on Making Decisions. New York: Wiley. 1-20. Print.

Kittrie, Orde F. (2016), *Lawfare: Law as a Weapon of War*. New York: Oxford UP. Print.

McConnell, P. (2013), "Systematic Operational Risk: The LIBOR Manipulation Scandal." *Journal of Operational Risk* 8.3: 59-99. Web. 08 Aug. 2016.

Scandizzo, S. (2005), Risk mapping and key risk indicators in operational risk management. *Economic Notes*, *34*(2), 231-256.

Shevchenko, P. V., M. G. Cruz, and G. W. Peters (2011), "OpRisk Data and Governance." *Fundamental Aspects of Operational Risk and Insurance Analytics: A Handbook of Operational Risk*. Hoboken: John Wiley & Sons. Pp 1-47. Print.

Tarullo, D. K. (2008), "Basel I." Banking on Basel: The Future of International Financial Regulation. Washington, DC: Peterson Institute for International Economics. Pp 45-85. Web. 12 Mar. 2016.